EXHIBIT QQ

LORD PETER HAIN

JUDICIAL COMMISSION OF INQUIRY INTO ALLEGATIONS OF STATE CAPTURE, CORRUPTION AND FRAUD IN THE PUBLIC SECTOR INCLUDING ORGANS OF STATE

2nd floor, Hillside House
17 Empire Road,
Parktown
Johannesburg
2193
Tel: (010) 214 to 0651
Email: inquiries@sastatecapture.org.za
Website: www.sastatecapture.org.za

INDEX: EXHIBIT QQ

#	Pages	Foot Note	File	Pages
	Submission by Lord Peter Hain	N/A	(a)	001 to 023
1.	Money-Laundering and Globalization, United Nations Office on Drugs and Crime	1	(a)	024 to 025
2.	State Capture wipes out third of SA's R4.9-trillion GDP	2	(a)	026 to 041
3.	Sanctions and Anti-Money Laundering Bill, Second Reading, Hansard, Volume 785, 1 November 2017	3, 4	(a)	042 to 050
4.	India's Bank of Baroda Played a Key Role in South Africa's Gupta Scandal	5, 6	(a)	051 to 065
5.	A thematic review of trust and company service providers	7	(a)	066 to 072
6.	United Kingdom, Transparency International	8	(a)	073
7.	KPMG South Africa executives dismissed over Gupta scandal - Financial Times	9, 10	(a)	074 to 076

#	Pages	Foot Note	File	Pages
8.	Ismail Momoniat - When will Bain tell the whole truth about its role at SARS	11	(a)	077 to 078
9.	Acacia Mining falls 4% on report of SFO probe	12	(a)	079
10.	Javelin throwing - Foot note	13	(a)	080
11.	Exclusive - Gupta-linked train company in R5bn rip-off - News24	14, 15	(a)	081 to 086
12.	N.Mokeshi (HOD FSHS) submission to Free State Provincial Legislature	16	(a)	087
13.	Pieter-Louis Myburgh, Gangster State Part III "the R1 Billion Housing Splurge"	17	(a)	088 to 141
14.	Guptas Big Banks Linked to South African-Chinese Locomotive Deal	18, 21	(a)	142 to 148
15.	Guptas 'laundered' R52m in Hong Kong, #StateCaptureInquiry told - IOL News	19	(a)	149 to 151
16.	How the Guptas Milked South Africa for Diamonds	20	(a)	152 to 158
17.	The house of Gupta	22	(a)	159 to 164
18.	Following Guptas' Temple Money-Laundering Trail - HuffPost UK	23	(a)	165 to 174
19.	Gupta wedding_ The most insane expenses for next week's R427m bash	24	(a)	175 to 180
20.	Spend £2.7bn more to tackle organised crime, says NCA chief - UK news - The Guardian	25	(a)	181 to 184
21.	SFO agrees first UK DPA with Standard Bank - Serious Fraud Office	26	(a)	185 to 188
22.	Economic Crime Plan 2019-22, HM Governmen and UK Fianance, July 2019	27, 28, 37, 40	(a)	189 to 264
23.	G20 High-Level Principles on Beneficial Ownership Transparency	29	(a)	265 to 267
24.	Financial Intelligence Centre Amendment Act	30	(a)	268
25.	The FATF Recommendations, International Standards on Combating Money Laundering & Financing of Terrorism and Proliferation	31, 44, 48	(a)	269 to 402

#	Pages	Foot Note	File	Pages
26.	Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001) South African Reserve Bank Act, 1989 (Act No. 90 of 1989)	32, 42	(a)	403
27.	South African Reserve Bank Act, 1989 (Act No. 90 of 1989)	33	(a)	404
28.	Corruption Watch	34	(a)	405
29.	Anti-Money-Laundering-the-SARs-Regime-Consultation-paper	35	(b)	406 to 627
30.	National Economic Crime Centre - National Crime Agency	36	(b)	628 to 631
31.	Eiti Standard 2019, The global standard for the good governance of oil, gas and minerals resources, 17 June 2019	38	(b)	632 to 703
32.	Clear signal to foreign investors - Hasty go ahead for Guptas to buy Optimum	39	(b)	704 to 716
33.	Prevention and Combating of Corrupt Activities (Act No. 12 of 2004)	41	(b)	717
34.	Azeri banker's high-spending wife targeted by new British anti-graft powers – Reuters	43	(b)	718 to 726
35.	Requests for Mutual Legal Assistance in Criminal Matters - Guidelines for authorities outside of the UK	45	(b)	727 to 781
36.	Justice ILR Extradition and Mutual Legal Assistance	46, 47	(b)	782 to 784
37.	Time up for the Guptas - Parliament approves extradition treaty with UAE - News24	49	(b)	785 to 788
38.	Letter dated 11 October 2019 from The Right Honourable Lord Hain of Neath to The Right Honourable Sajid Javid MO	N/A	(b)	789 to 790
39.	Letter dated 05 November 2019 from The Foreign & Commonwealth Office (Mr Andrew Stephenson MP) to The Right Honourable Lord Hain of Neath	N/A	(b)	791 to 792

31 October 2019

LORD PETER HAIN

SUBMISSION TO THE JUDICIAL COMMISSION OF ENQUIRY INTO STATE CAPTURE

THE GLOBAL DIMENSION

INTRODUCTION

1. State capture in South Africa was in part facilitated by the massive complicity of international financial institutions, global corporates and foreign governments (notably in India, Dubai and Hong Kong). These governments and corporates must now act in partnership with the South African Treasury to recover the billions of rands looted from SA taxpayers, much laundered abroad. Having spoken under parliamentary privilege in the UK House of Lords in September 2017 – January 2018 on these matters, on the basis of interaction with whistle-blowers within the South African state and private sectors, my focus is upon the global dimension (especially money laundering) because without that state capture could not have been as monumentally lucrative to its perpetrators as it so tragically has been.

2. It is incumbent upon the relevant foreign governments implicated and their enforcement and regulatory agencies to resource and prioritise cooperation to bring to justice those responsible for the international looting from South African taxpayers. The same must be the case for the global corporates involved. But, so far, neither has happened.

3. I am grateful for their advice and assistance in drafting this to a number of friends and contacts for their expertise without which my submission could not have been anything as comprehensive and also I hope authoritative.

STRUCTURE OF REPORT

4. This report starts by providing an overview of the *Current Status of Financial Crime Globally.* Following that introduction, *Part One* explains the roles and importance of international actors and foreign enablers, without whom there could not have been the state capture of South Africa, drawing primarily on the well-known case-studies of Messrs Ajay, Atul and Rajesh Gupta's (the Guptas) corrupt activities. *Part Two* recommends practical, specific and achievable steps that should be taken by international enablers (such as banks and consultants, foreign states and enforcement agencies) as well as South African authorities to prevent future state capture and to help make amends for the harm they have contributed to. Finally, the *Conclusion* provides an overview of the key points in this report and the principles of transparency and fairness that it embodies.

Description	Page Reference
CURRENT STATUS OF FINANCIAL CRIME GLOBALLY	
Global picture	3
South African picture	3-4
PART ONE: INTERNATIONAL ACTORS – CONDUCT CONTRIBUTING TO SOUTH AFRICA'S STATE CAPTURE	
Banks	5-6
Professional Enablers	6-7
Corporates	8
States	9-10
PART TWO: REMEDIAL MEASURES	
Banks and Professional Enablers • Transparency of Ownership • Information Sharing • Self-policing	11-15
Corporates • Extractive Industries Transparency Initiative • Black Economic Empowerment	16-17
States • Legislation • Financial Action Task Force • Mutual Legal Assistance • Extradition	18-21
CONCLUSION	
Conclusion • Transparency and Fairness	22

CURRENT STATUS OF FINANCIAL CRIME GLOBALLY

Global Picture

5. Financial crime threatens the security and prosperity of the international community and the global financial network. It undermines the integrity of financial systems and damages the international reputation of the states where it flourishes. Criminals launder vast sums of illicit funds every year; transforming their ill-gotten gains in to seemingly legitimate assets. It is estimated that around 5% of global GDP or USD 2 trillion is laundered each and every year.[1] Developing countries seem particularly prone to forms of corruption and the abuse of their domestic financial and regulatory systems. They are also particularly unable to navigate the web of global money flows, or to enforce reasonable standards of transparency and fairness in international business and banking. The impact of these combined issues leaves many countries without the levers to prevent flows of illicit funds from their economy and so keeps many of their citizens in perpetual and abject poverty.

6. Fighting corruption therefore requires global action and global co-ordination from a range of stakeholders, including governments, businesses, banks and non-governmental organisations. Without this, the state capture of South Africa or another country will happen again, the South African Treasury will not be able to recover the billions looted and laundered abroad, and 'rent seeking' enabled by international banks and multinationals in South Africa will be able to continue largely unhindered and undeterred.

South African Picture

7. Whilst the true scale of the flagrant theft from the South African state (and therefore the South African taxpayers) under the Zuma administration is not fully known, the direct and indirect costs of state capture have been estimated at around R1.5 trillion.[2]

8. The Commission of Inquiry into State Capture (the Commission) is already well aware of the systemic lack of transparency and accountability of South African government bodies that allowed corruption to thrive, provided criminals with access to the Treasury's coffers and supplied the foundations for state capture. Whilst South Africa must reflect on the domestic changes it needs to make as a nation to prevent corrupt individuals infiltrating public offices and looting from the South African people, it is also crucial that the international community fully acknowledges the roles that various international actors played in the capture of the state. It was international actors who helped and continue to help corrupt individuals to enjoy the spoils of their illegality by offering them the means to move their ill-gotten gains out of South Africa, and then sometimes (as in the Estina dairy farm scandal) back in undetected. It was international actors who helped corrupt individuals create complex corporate structures disguising the true ownership of funds and complicating the tracing and repatriation of stolen funds whilst earning fat fees out of the looting. It was international actors that provided refuge to corrupt individuals and the means to continue their activities through less regulated 'open' economies.

9. Therefore, international actors across the public and private sectors must commit their resources to strengthening regulations, improving corporate governance, increasing transparency and coordinating globally to reduce financial crime. They should also

---

[1] *Money-Laundering and Globalization*, United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/money-laundering/globalization.html

[2] https://www.dailymaverick.co.za/article/2019-03-01-state-capture-wipes-out-third-of-sas-r4-9-trillion-gdp-never-mind-lost-trust-confidence-opportunity

actively assist the South African authorities in the quest to recover and return the stolen funds to South Africa. Without cross-border cooperation and engagement of the public and private sectors, no country will be emancipated from financial crime.[3]

[3] *Sanctions and Anti-Money Laundering Bill*, Second Reading, Hansard, Volume 785, 1 November 2017, https://hansard.parliament.uk/Lords/2017-11-01/debates/B122FCEA-07C2-4A5E-A5DC-87EB70642A5E/SanctionsAndAnti-MoneyLaunderingBill(HL)#contribution-A31355C8-48D9-441F-B8C2-99717600C294

PART ONE: INTERNATIONAL ACTORS – CONDUCT CONTRIBUTING TO SOUTH AFRICA'S STATE CAPTURE

10. In this part 1, I describe how international actors have (whether knowingly or unknowingly) facilitated State Capture in South Africa. The cases that I cite in this regard are drawn from reports in the public domain and from evidence submitted to this Commission of Inquiry. Save where I refer to my own interactions with the relevant international actors, I do not claim to have direct personal knowledge of the facts in this regard and rely on the reports and evidence cited in the footnotes to this report.

Banks

11. Electronic banking remains the simplest and fastest means of transferring funds between people and across borders. It allows criminals to move their money to more convenient (often also less regulated) jurisdictions and it 'cleans' the money by mingling it with other funds and disguising its source so that it is easier to spend.

12. It is alleged that the Guptas used a number of international banks (many of whom are household names, including HSBC4, Standard Chartered and, above all, Bank of Baroda) to transfer money around their network, disguise payments and hide the source of their funds. Broadly, the banks appear to have assisted the Guptas in two ways: (i) by allowing bank accounts to be opened and in doing so granting access to the bank's global network; and (ii) by allowing the transfer of illicit funds into and out of accounts. There were, however, warning clear signs even in publicly available materials that the Guptas' activities were suspicious and these 'red flags' should have been spotted by the banks either much sooner or immediately:

    12.1 the secretive nature of the transactions (the reason, the source of funds and the ownership of the accounts was often obscured);

    12.2 there were unexplained payments to and from third parties with little or no apparent connection to the underlying transaction;12.3 many accounts were used to transfer funds of various amounts around shell companies (or front companies, which do not conduct trading but allow funds to flow through them, while obscuring the persons who control them);

    12.4 there were unexplained connections with and movement of monies between jurisdictions;

    12.5 the Guptas (who beneficially owned most of the companies) were linked to the corrupt political elite under former President Jacob Zuma in South Africa and there was an increasing awareness amongst the international community that corruption was rife in South Africa under the Zuma administration; and

    12.6 the legitimate funds created by the Gupta's enterprises were dwarfed by the funds they amassed through illegal activity.

13. A specific example of a transaction that should have been stopped, or at the least investigated by the bank concerned, was a loan on 18 January 2017 by Trillian Management Consulting (then majority owned by a Gupta associate; Salim Essa) of

[4] For example, HSBC's activities in South Africa have been the subject of press reports and my own UK parliamentary intervention (see, *Sanctions and Anti-Money Laundering Bill*, Second Reading, Hansard, Volume 785, 1 November 2017, https://hansard.parliament.uk/Lords/2017-11-01/debates/B122FCEA-07C2-4A5E-A5DC-87EB70642A5E/SanctionsAndAnti-MoneyLaunderingBill(HL)#contribution-A31355C8-48D9-441F-B8C2-99717600C294)

R160 million to Centaur Mining (a Gupta owned company) via Trillian Financial Advisory (a Gupta owned company).[5] It is alleged that Bank of Baroda SA (part of India's state-owned, global Bank of Baroda) bank accounts were utilised for this movement of funds. The reason for this chain of transactions was stated to be an inter-company loan. However, no loan documentation has so far been found to exist and no explanation was reportedly provided to the bank for the structure of the transaction.[6] Other reports into the activities of this branch of the bank in respect of Gupta associated accounts and transfers indicate that it issued loan guarantees without approval and may have quashed internal compliance concerns raised by employees.

14. In another example, it has been alleged that South African government funding for a state financed project (Estina Dairy Farm) was transferred via the Gupta controlled Estina (Pty) Ltd to a Standard Chartered bank account held by Gateway Limited (a Gupta owned company registered in the United Arab Emirates) in May, August, September 2013. Standard Chartered did not stop this transaction despite the fact that government funds were leaving the jurisdiction to a company beneficially owned by the Guptas with no material explanation provided regarding the suspicious payment structure.

15. Given that banks ought to have access to customer data and transaction data for all accounts they open and transfers they facilitate, they are well placed to monitor the legitimacy of any and all transactions, in addition to having regulatory and moral responsibilities to recognise and stop illegal money flows. But when they met me in London (after I had named them under parliamentary privilege in November 2017 as complicit in state capture/money laundering), I found a great reluctance from HSBC and Standard Chartered – citing 'client confidentiality' – to cooperate fully when I specifically asked them to trace and track the money laundered by the Guptas under the Zuma administration. That is simply unacceptable.

16. It is important that banks take full responsibility for monitoring transactions and for ensuring that adequate compliance policies and procedures are properly implemented across all business areas and branches to prevent money launderers from disguising and disseminating their illegal profits and exploiting weaknesses within the banks' infrastructure.

The suggested remedial measures in relation to banks are considered in *Part Two – Banks and Professional Enablers* below (pages 11-15).

Professional Enablers

17. Professional enablers are persons or entities that become involved (whether intentionally or unintentionally) in facilitating the 'cleaning' of laundered money in return for a fee. Their role is to disguise the source, location and ownership of funds. Examples of professional enablers include lawyers, auditors/accountants and estate agents. Lawyers might assist by setting up complex corporate structures of shell companies enabling money to be moved from one country to another country where there is low transparency. Accountants might incorrectly audit company financials

[5] *India's Bank of Baroda Played a Key Role in South Africa's Gupta Scandal*, Organized Crime and Corruption Reporting Project, 27 February 2018, https://www.occrp.org/en/investigations/7696-india-s-bank-of-baroda-played-a-key-role-in-south-africa-s-gupta-scandal

[6] *India's Bank of Baroda Played a Key Role in South Africa's Gupta Scandal*, Organized Crime and Corruption Reporting Project, 27 February 2018, https://www.occrp.org/en/investigations/7696-india-s-bank-of-baroda-played-a-key-role-in-south-africa-s-gupta-scandal

leading to suspicious transactions being hidden in the accounts. Estate agents might receive laundered money into their client accounts during property purchases.

18. To provide insight into the scale of this problem, the Solicitors Regulation Authority (SRA) in the UK completed a review of whether 59 law firms in England and Wales were meeting their obligations to conduct money laundering checks. 26 of those 59 firms were ultimately referred into disciplinary processes.[7] If the situation is this poor in a country that otherwise scores well on anti-corruption by other measures (e.g. the UK has a low ranking of 11th in Transparency International's annual Corruption Perception Index[8]) what does that suggest about the anti-money laundering capability of professional enablers in countries with a worse reputation?

19. As is set out in detail below, a number of professional enablers appear to have, or have themselves recognised that they assisted the Guptas in their looting from the South African people, including global brand names such as KPMG, Bain & Co and Hogan Lovells. The relevant allegations are to the effect that these firms profited while the Guptas hid funds stolen from South Africa; funds that would otherwise have been spent on essential public services and on helping to repair the colossal damage caused by the apartheid, still a huge deadweight on the country..

20. In 2018, I referred Hogan Lovells to the SRA for whitewashing corruption within the South African Revenue Service, requesting it be disbarred from practicing in the UK for its terrible complicity in state capture. But the SRA eventually accepted Hogan Lovells' own defence that it was only the international law firm it claimed to be for 'branding purposes', and that the SRA therefore had no locus to intervene in the reported corruption collusion of its South African branch. I note that Hogan Lovells has since deservedly lost South African business and been forced to restructure after it refused to admit obvious culpability, even when other global corporates did.

21. Another example of a professional enabler who assisted the Guptas is KPMG's South Africa Division. KPMG South Africa was responsible for auditing various Gupta companies in South Africa for around 15 years up until March 2016.[9] During that period, it flagrantly ignored warnings regarding the integrity and ethics of the Guptas and falsely categorised spending (such as a wedding in 2013) as business expenses whilst earning significant fees for performing auditing services (such fees ultimately being paid for by laundered funds). Eventually the firm conducted an internal investigation which led to eight senior executives being fired and a promise to repay R40 million it had earned from auditing Gupta related companies to anti-corruption charities.[10]

22. A third example is that of Bain, the Boston-based consultancy firm, which was named in the Commission of Inquiry into Tax Administration and Governance by the South African Revenue Service (referred to as the "Nugent Commission") as having 'coached' Tom Moyane on how to implement the capturing of SARS a full year before he was appointed Commissioner. Several of these meetings took pace at Nkandla, the private homestead of President Zuma. "So serious were its actions that the Nugent commission recommends criminal prosecutions against Bain & Co. It found that Bain had engaged in a "premeditated offensive against SARS, strategised by the

---

7 *A thematic review of trust and company service providers*, Solicitors Regulation Authority, May 2019, http://www.sra.org.uk/sra/how-we-work/reports/aml-thematic-review.page

8 *United Kingdom*, Transparency International, https://www.transparency.org/country/GBR

9 *KPMG South Africa executives dismissed over Gupta scandal*, Financial Times, 15 September 2017, https://www.ft.com/content/ce8ddb84-9a01-11e7-a652-cde3f882dd7b

10 *KPMG South Africa executives dismissed over Gupta scandal*, Financial Times, 15 September 2017, https://www.ft.com/content/ce8ddb84-9a01-11e7-a652-cde3f882dd7b

local office of Bain & Company Inc, located in Boston, for [former SARS head] Mr [Tom] Moyane to seize SARS … Mr Moyane's interest was to take control of SARS. Bain's interest was to make money."[11]

23. Professional services firms have access to client data, meaning that they are well placed to monitor and recognise suspicious transactions and customer activities. It is essential that global professional services firms enact robust compliance policies and procedures to recognise and prevent money-laundering and actively educate all employees across all business areas and branches about the importance of those policies.

The suggested remedial measures that should be implemented in relation to professional enablers are considered in the *Part Two – Banks and Professional Enablers* section below (pages 11-15).

Corporates

24. Allegations of corruption are often directed at the state and government officials. However, South Africa is a living example of where privately owned companies can become intentional or unintentional facilitators of money laundering and bribery by doing business with criminals in order to win lucrative contracts or other commercial advantages, often in the state procurement space. Conduct of this nature has prompted many an investigation by a regulator, such as the UK's Serious Fraud Office's discussions with Acacia Mining in December 2018 in relation to employees in Tanzania engaging in corruption.[12]

25. A common typology of how a company might facilitate corruption (and commit criminal offences in doing so) is where a corrupt individual (such as a government official) offers a company a public contract in return for a commission payment (also known as 'rent seeking' and a form of bribery).[13] In this scenario the company, frequently under the guise of a Black Empowerment Enterprise (BEE), is awarded a private or government contract at an agreed price (often an inflated amount to take into account various bribery payments to government officials and associates) without either (a) having to complete a fair bidding process (discouraging fair competition) or (b) having to prove their capability leading to contracts being awarded to parties who do not have the capability to fulfil them. Contracts infected with this form of corruption are rarely performed properly or even sometimes at all; even where the contract is effectively 'sold' to an ostensibly competent foreign company. Examples of this type of corruption are set out below.

26. *Transnet* – Its senior executives assisted the Guptas in corrupting the state procurement process for commercial gain. In a contract obtained for providing locomotives South China Rail undertook to pay more than £250 million in bribes to

---

[11] https://www.businesslive.co.za/bd/opinion/2019-07-01-ismail-momoniat-when-will-bain-tell-the-whole-truth-about-its-role-at-sars/

[12] *Acacia Mining falls 4% on report of SFO probe*, Financial Time, 17 December 2018, https://www.ft.com/content/7d585320-01f2-11e9-9d01-cd4d49afbbe3

[13] In South Africa a variant of this private-state collaboration in corruption is referred to as 'javelin-throwing', where corrupt officials sign off on a lucrative tender, knowing that they will be leaving the employ of government in the near future and that they will become part of the benefitting company either as a director or as a senior employee.

Gupta linked shell or BEE companies in return for the Guptas using their political influence to ensure that the Transnet tender was awarded to South China Rail.[14] It was later revealed that South China Rail did not adhere to the strict local content and supplier development obligations, required to assist in growing the South African economy. For the first 166 locomotives delivered, the local content score was 33%.[15]

27. *Housing* - In the Free State under the leadership of the then ANC Premier, Mr Ace Magashule, an alleged associate of the Guptas, the absence of 11,000 homes for those in dire need[16] has been explained as a direct result of building contracts being awarded to political supporters through BEE's, where those BEE's all too frequently had no or little building experience and would have failed any transparent or fair procurement process.[17]

28. *Consultants* - The capture of the South African state would not have occurred if companies had refused to engage in negotiations and broker deals with corrupt government officials and associates. Yet many, including global brand names like SAP and McKinsey appear shamelessly to have done so, earning enormous fees and thereby being complicit in the looting and diversion of scarce taxpayers money from providing much needed health, education, care, housing and other vital provisions in a country still weighed down by the apartheid legacy of mass unemployment, poverty and deliberate under-skilling.

29. The private sector is legally responsible for fostering an environment where financial crime does not pay and where there is fair competition for tenders and contracts. Creating such an environment requires companies to know and understand who they are doing business with, whether that is a counterparty, a consultant or a supplier, have access to information to ascertain whether a counter-party (including BEE's) is capable of completing its obligations and to have confirmation of whether a party and its owners are located in South Africa, the UK or anywhere else in the world.

The suggested remedial measures that should be implemented in relation to corporates are considered in *Part Two - Corporates* section below (pages 16-17).

States

30. Globalisation has made it easier for criminals to dissipate tainted funds more broadly; resulting in countries unconnected to the underlying crime being used to launder money and being drawn into the web of corruption. Without the cooperation and coordination of states, criminals are able to simply avoid the rule of law by relocating themselves and their stolen funds to another country. Criminals often exploit the differing standards and enforcement of legislation across states, and the lack of political will in some states to fund the fight against financial crime as a result of budgetary constraints, by choosing to locate assets in jurisdictions where regulations are weaker, regulators are underfunded, or where there is less transparency around corporate ownership.

31. Many criminals also attempt to relocate to countries where there is no extradition agreement in place to avoid being forced to return to the country where their crimes were perpetrated. Up until now, governments have paid lip service to curbing financial

---

[14] *Gupta-linked train company in R5bn rip-off*, News24, 23 March 2018, https://www.news24.com/SouthAfrica/News/exclusive-gupta-linked-train-company-in-r5bn-rip-off-20180323

[15] *Gupta-linked train company in R5bn rip-off*, News24, 23 March 2018, https://www.news24.com/SouthAfrica/News/exclusive-gupta-linked-train-company-in-r5bn-rip-off-20180323

[16] N.Mokeshi (HOD FSHS) submission to Free State Provincial Legislature, 4 August 2015

[17] Pieter-Louis Myburgh, *Gangster State* (Penguin, 2019), chapter three "the R1 Billion Housing Splurge"

crime without actually doing so. The UK and South Africa, for example, both have strict anti-money laundering regulations but the named wrongdoers and many others have managed to evade this legislation with the complicity of South African public officials and the 'professional services' of foreign headquartered or located global banks and professional enablers, respectively.

32. An example of the global reach of the Guptas and their utilisation of other states to safeguard their wealth and prevent their arrest is their links to Dubai (where they currently reside), India (their country of birth where they also reside) and Hong Kong (where they reportedly funnelled laundered funds and received kickbacks).[18]

33. *Hong Kong* - Shiwa Mazibuko, head of the South Africa Reserve Bank financial surveillance department informed the Commission during his testimony on 7 June 2019 that around R52 million was moved from South Africa to Hong Kong via Homix (a Gupta owned company) to Morning Star International and YKA International Trading Company (Hong Kong companies).[19] Other reports indicate that some of the funds laundered in Hong Kong were used to purchase diamonds via companies such as Simoni Gems (a Hong Kong company linked to the Guptas that received funds from South African Gupta companies).[20] These funds have not yet been repatriated to South Africa, nor have the Hong Kong authorities taken any public action against the Guptas. Other reports indicate that more than $100 million of the kickbacks received by the Guptas in respect of purchases of CSR and CNR locomotives by Transnet were channelled through the HSBC Hong Kong accounts of their front companies Tequesta and Regiments Asia.[21]

34. *Dubai* - The Guptas currently reside in Dubai (Villa L35, Lailak Street, Emirates Hills, Dubai, identifiable by the Gupta gold crest at the entrance gates and purchased with laundered funds)[22] after fleeing from South Africa in early 2018. The Guptas have not yet been extradited to face trial in South Africa, nor have any monies in Dubai been repatriated to South Africa.

35. *India* – The Guptas are Indian by birth and have a number of family members, businesses and properties in India. The Guptas have also commissioned the building of the R200 million Shiva Dham temple using laundered funds and appear to continue haemorrhaging funds at an alarming rate, including recently funding a wedding costing R427 million in June 2019.[23,24] Whilst the Indian authorities have investigated the Guptas, no funds have yet been repatriated to South Africa.

36. The active assistance and determined cooperation of diplomats and states is critical to the repatriation of South Africa's stolen funds and the extradition of the Guptas to face trial in South Africa for their crimes. States must also strengthen regulations and

---

[18] https://www.occrp.org/en/investigations/7257-guptas-big-banks-linked-to-south-african-chinese-locomotive-deal

[19] *Guptas "laundered" R52m in Hong Kong, #StateCaptureInquiry told*, IOL, 8 June 2019, https://www.iol.co.za/news/politics/guptas-laundered-r52m-in-hong-kong-statecaptureinquiry-told-25550308

[20] *How the Guptas Milked South Africa for Diamonds*, Organized Crime and Corruption Reporting Project, 23 August 2018, https://www.occrp.org/en/investigations/8500-how-the-guptas-milked-south-africa-for-diamonds

[21] https://www.occrp.org/en/investigations/7257-guptas-big-banks-linked-to-south-african-chinese-locomotive-deal

[22] *house of Gupta*, SA Journalist, https://sajournalist.atavist.com/the-house-of-gupta

[23] *Following the Guptas' Temple Money-Laundering Trail*, Huffington Post, 9 April 2018, https://www.huffingtonpost.co.uk/2018/04/09/following-guptas-temple-money-laundering-trail_a_23406525/?ncid=other_email_o63gt2jcad4&utm_campaign=share_email

[24] *Gupta wedding: These are the most insane expenses for next week's R427m ceremony*, The South African, 12 June 2019, https://www.thesouthafrican.com/lifestyle/where-is-gupta-wedding-auli-how-much-expenses/

enforce them within their jurisdictional reach to ensure that there is a real deterrent from engaging in illegal activity. It is not enough to establish legislation such as the UK's Bribery Act 2010 and South Africa's own powerful anti-corruption legislation. Enforcement and investigative agencies (such as the Serious Fraud Office, National Crime Agency and Financial Conduct Authority in the UK, Directorate for Priority Crime Investigation within the SA Police Services and the National Prosecuting Authority and the Special Investigations Unit in South Africa) need to be utilising the legislation to conduct investigations and require proper resourcing to do so. In the UK, these agencies have not had anything resembling the resources required to combat financial crime in recent years, leading to a request earlier this year from the head of the National Crime Agency for an additional GBP 2.7 billion in funding for that agency alone.[25] As a reminder of the assistance these agencies can provide in combating financial crime, the UK's Serious Fraud Office's investigation into the activities of Standard Bank Plc in Tanzania led to USD 7 million being paid in compensation to the Government of Tanzania and over USD25 million paid in fines and disgorgement of profits.[26]

37. States simply cannot continue to condemn corruption on the international stage whilst allowing the proceeds of crime to be pumped into and through their economies. In particular, the states referred to above must reflect on their involvement in the capture of South Africa and implement remedial steps as a matter of urgency.

The suggested remedial measures that should be implemented in relation to states are considered in *Part Two - States* section below (pages 18-21).

[25] *Spend £2.7bn more to talk organised crime, says NCA chief*, The Guardian, 14 May 2019, https://www.theguardian.com/uk-news/2019/may/14/spend-27bn-more-to-tackle-organised-says-nca-chief

[26] *SFO agrees first UK DPA with Standard Bank*, Serious Fraud Office, 30 November 2015, https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-dpa-with-standard-bank/

PART TWO: REMEDIAL MEASURES

38. The consequences of South Africa's crippling state capture demonstrate the need for the international community to re-affirm its collective commitment to preventing and eradicating financial crime. As explained in Part One, without the involvement of international actors and enablers, the devastating impact financial crime wrought on South Africa would have been significantly reduced. We must now treat South Africa's experience of state capture as an opportunity; an opportunity for the international community, including business and banking, to learn from the failures and weaknesses in the global regulatory system that enabled such stifling corruption to eventuate. Specific steps can and must be taken to prevent state capture afflicting South Africa or any other country in the future.

39. The following recommendations are made to foster a transparent international environment where there is pro-active co-operation between banks, professional enablers, companies and states, and where the perpetrators of corruption and money laundering are no longer able to hide in the shadows.

Banks and Professional Enablers

40. Successfully combating financial crime can only be achieved through a meaningful partnership between the private sector and the public sector, concentrating around shared strategic priorities and the alignment of resources.[27] Within the private sector, banks and professional enablers have arguably the most significant role to play in combatting financial crime. It should be a source of shame for the world's leading economies that banking institutions and professional enablers responsible for facilitating corrupt practices in foreign countries are headquartered in their jurisdictions (London, New York, Delhi and Shanghai, for instance). I note that the average, honest citizen on a modest or medium income is subject to all manner of frustrating and time-consuming procedures and requirements to open a bank account or legitimately move money, but somehow banks turn a blind eye to global crime such as that perpetrated by the Guptas, their cronies and allies, on a gargantuan scale. How can that be right?

41. Whilst it might seem counterintuitive to seek assistance from entities that are reported to have contributed to state capture and assisted corrupt persons to move stolen funds out of South Africa (for instance HSBC, Standard Chartered, Bank of Baroda, McKinsey, KPMG, Hogan Lovells, and Bain & Co, to name a few), their involvement is crucial to understanding the global picture of financial crime. For it is a fact that funds moved across the world today leave a digital footprint. Banks and professional enablers (particularly global banks) possess the technological and financial clout needed to force change and that power should be harnessed to assist regulators to target their often too limited resources.

Transparency of Ownership

Recommendation: (i) creation of a public register of beneficial owners (BOs) within the next six months; and (ii) strengthening the audit programme of banks and professional enablers' due diligence in South Africa

42. In order for banks and professional enablers to recognise suspicious customers or transactions, they must know the identity of the customer. Understanding who the beneficial owners (BOs) of corporate entities are is integral to enabling banks and

[27] *Economic Crime Plan 2019-22*, HM Government and UK Finance, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf

professional enablers to understand the background to a transaction so that a proper assessment can be made of whether there is a corruption risk.[28] This is why greater transparency around beneficial ownership has been high on the G20 Agenda for the last five years, after G20 leaders adopted the *High-Level Principles on Beneficial Ownership Transparency* in 2014.[29] In this regard, South Africa has recently introduced legislation to strengthen customer due diligence measures, including with respect to beneficial ownership and persons in prominent positions.[30]

43. As explained in *Part One*, criminals often hide behind complex layers of shell companies, obstructing banks and professional enablers from associating transactions to or from the shell companies with the criminal. Banks and professional enablers therefore need to ensure that thorough due diligence is carried out before customers are on-boarded (e.g. before bank accounts are opened or clients accepted) to ensure that they understand the true identity of the customer. Once on-boarded, banks and professional enablers should conduct ongoing monitoring of the customer to ensure that the corruption risk profile is updated to reflect any new information received.[31] This is particularly important in relation to business areas (such as state procurement) or geographical areas (such as South Africa) that have experienced a high risk of corruption which was rife under the Zuma Administration, or where the customer is a politically exposed person. In these higher risk scenarios, more rigorous requirements should be adopted accordingly.

44. In order to facilitate banks and professional enablers identification of BOs, states should commit to increasing transparency around the parties that enter into contracts with state-owned enterprises by creating a public BO register within the next six months containing information (name and address) for all of the BOs of all the entities that have entered into major contracts with the South African government (above a certain threshold amount). This would help banks and professional enablers to assess the legitimacy of payments from state-owned enterprises to third parties. Once live, BO information for new major contracts should be added as a matter of course and in advance of any contract being signed so that the BO information can be scrutinised. The register should also be updated and verified by an independent body on a monthly basis to ensure that banks and professional enablers (and others) have access to accurate and up-to-date information, and to prevent the register being fraudulently completed by corrupt officials.

45. In order to ensure that banks and professional enablers are held to account for their risk assessments of customers and transactions, it is recommended that the programme for auditing the due diligence carried out by these entities in South Africa is improved. Currently, the South African Reserve Bank audits banks on a regular basis under the Financial Intelligence Centre Act 2001[32] and the South African Reserve Bank Act, 1989.[33] Reports on the audits are then published and substantial fines

---

[28] *Economic Crime Plan 2019-22*, HM Government and UK Finance, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf

[29] *G20 High-Level Principles on Beneficial Ownership Transparency*, G20, Australia 2014, http://www.g20.utoronto.ca/2014/g20_high-level_principles_beneficial_ownership_transparency.pdf

[30] *Financial Intelligence Centre Amendment Act*, Act 1 of 2017

[31] *The FATF Recommendations*, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Adopted by the FATF Plenary in February 2012 and updated in June 2019, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[32] *Financial Intelligence Centre Act*, 2001 (Act No. 38 of 2001), https://www.fic.gov.za/Documents/FIC%20Act%20with%202017%20amendments%20(1)%20(1).pdf

[33] *South African Reserve Bank Act*, 1989 (Act No. 90 of 1989) Regulations Relating to the South African Reserve Bank, https://www.gov.za/sites/default/files/gcis_document/201409/33552808.pdf

imposed for non-compliance. Given the significant role that banks and professional enablers played in facilitating state capture, it is suggested that the South African Reserve Bank carries out a greater number of audits on these entities, particularly on those that have been identified as not complying with anti-money laundering legislation previously. These audits should take place without notice and a random sample of due diligence files should be reviewed, thereby making it difficult for banks and professional enablers to hide any compliance failures. Finally, key findings from these reviews (to the extent they do not assist criminals seeking to beat bank's controls), a 'root causes analysis' and an overall score should be made publicly available, as should personal undertakings by senior 'headquarter' management to timelines and funding; guaranteeing commitments made by the relevant bank's local branch to any critical remediation work. In this way the public, business and government can be helped to reach their decisions about which banks live up to their ethical claims and deserve increased business.

Information Sharing

46. **Recommendations: (i) consolidation of data within banks and professional enablers; (ii) establish a body replicating the UK's Joint Money Laundering Steering Group (JMLSG) within South Africa within the next 12 months; (iii) implement legislation allowing the voluntary sharing of data between banks where there is a suspicion of money laundering; (iv) establish a body replicating the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) in South Africa within the next 12 months; and (v) require banks to provide the South African regulators with a copy of monthly reports to management on corruption risks**

47. Significant advances in technology have made it easier than ever to collate, store and share data. However, fragmentation of domestic and cross-border information sharing (i) within banks and professional enablers; (ii) between banks and professional enablers; and (iii) between banks and professional enablers and states, continues to impede financial crime prevention and prevent those parties from understanding the full financial crime picture. Greater (and better quality) data sharing will enable banks and professional enablers to identify and stop suspicious transactions and to more accurately report the nature of suspicious transactions to regulators, which in turn will help regulators to identify criminal activity and prioritise enforcement.

48. Corruption Watch (part of Transparency International focusing on fighting corruption in South Africa) has assisted in shining light on the corrupt activities taking place in South Africa by raising and maintaining public awareness of what corruption looks like and how it affects ordinary people's lives.[34] However, the engagement of civil society alone is not sufficient to understand the true scale of financial crime.

49. Banks and professional enablers (in particular global banks) are crucial to building an accurate picture of financial crime because they have access to software and systems that enable them to retain and collate information on customers and transactions that are unavailable to a regulator in the ordinary course. Similarly, banks often have access to huge financial resources and employ large teams of compliance personnel to assess financial crime risks that underfunded regulators may only dream of. Therefore, banks and professional enablers are the first line of defence when it comes to corruption and a private-public sector partnership is integral to reducing financial crime. Although some sharing of information already occurs, it is not effective and Banks must cease hiding behind confidentiality (or the limits of current reporting systems), and work collaboratively and pro-actively to share useful data and

[34] *Corruption Watch*, https://www.corruptionwatch.org.za/

intelligence on a confidential basis with South Africa, global regulators and enforcement agencies.

50. It is moreover also incumbent on states to recognise the value of sharing information with and amongst banks. It is a frequent complaint of banks that they rarely receive feedback from regulators regarding the quality of their reporting. They seldom receive any indication of whom regulators have identified as targets of suspicion and are not called upon to assist in the monitoring of their transactional behaviour. It is important that regulators develop better forms of cooperation with banks and trusted working relationships.

Within Banks and Professional Enablers

51. Banks and professional enablers must consolidate data across their organisations (i.e. information should be shared across different product departments and geographical areas). This will help prevent 'passporting', whereby criminals gain access to a financial institution's multinational network through a less regulated jurisdiction or product area. Banks and professional enablers should not be allowed to claim ignorance of the activities of branches placed in jurisdictions in a bank's multinational operations where anti-money laundering policies and procedures are not as rigorous, or where there are opaque banking and corporate structures. We need to look no further than the activities of the South African branch of Bank of Baroda (see *Part One – Banks* above) for an example of how a local bank branch was exploited to gain access to a global bank's infrastructure.

52. Banks and professional enablers must commit to ensuring that they are diligently consolidating and reviewing the data they obtain on customers and transactions across the network so that employees have access to all of the data on a customer or a transaction and can judge the financial crime risk (and report to the regulators) accordingly.

Between Banks and Professional Enablers

53. In order to encourage information sharing between banks and professional enablers so that they can create a more complete picture of a customer and their transactions, it is recommended that a body replicating the UK's Joint Money Laundering Steering Group (JMLSG) is set up within South Africa in the next 12 months. JMLSG (made up of the leading UK trade associations in the financial services industry) has created practical guidance for the financial sector around how banks should fulfil their obligations under UK anti-money laundering and counter terrorist financing laws and regulations. This guidance has reportedly significantly enhanced the ability of those in the financial sector to comply with the applicable laws and regulations because it is written by those with an in-depth knowledge of how that sector works on the ground. It has also ensured that there is a degree of universality in approach across the financial sector.

54. It is further recommended that legislation permitting the voluntary sharing of data between banks where there is a suspicion of money laundering should be implemented in South Africa, as has occurred in other states. For example, the UK's Criminal Finances Act 2017 introduces voluntary information sharing between regulated entities (such as banks and professional enablers) when they have notified the UK's National Crime Agency of a suspicion of money laundering. These provisions have allowed banks and professional enablers to communicate when there is a suspicion of money laundering and collate the relevant data held by multiple organisations so that they can provide a more fulsome picture to regulators (enabling the regulator in turn to better

allocate resources and make a more accurate assessment as to what action needs to be taken in respect of the transaction). [35]

Between Banks and Professional Enablers and States

55. In order to foster relations between state law enforcement and the financial sector, it is recommended that South Africa establishes a body replicating the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) within the next 12 months. JMLIT promotes the exchange and analysis of information relating to money laundering and wider economic threats and, since its inception, has supported and developed over 500 law enforcement investigations and has directly contributed to over 130 arrests and the seizure or restraint of over £46m m.[36] As is the case for JMLIT, this newly formed body should be comprised of both local banks and international banks (in recognition that corruption and money laundering can involve the global movement of funds around banking institutions).

56. It is further recommended that international banks should be required to share, with the South African authorities, copies of their monthly or weekly reports to management relating to their assessment of money-laundering, sanctions and corruption risks within the bank and the effectiveness of the banks' compliance programme (in their unedited form). These reports, which are already required to be created by US and UK authorities (even if they are not shared), would enable the authorities to better understand how robust the bank's compliance programme is within South Africa against the inherent risk and whether there are any material weaknesses that criminals might exploit. Collating key themes from these reports would also provide an overview in almost real time which would help the South African agencies target limited resources. There is simply no good reason for foreign banks to be better informed of the financial crime risk they present to South Africa, than the South African authorities.

Self-policing

57. Recommendation: Additional penalties for banks and professional enablers for failure to self-monitor (removal or suspension of banking licenses and a 'senior manager's regime')

58. In addition to banks and professional enablers sharing data, these organisations must make better use of the data they have access to by fastidiously ensuring that it is utilised to identify potential criminal activity. Banks and professional enablers should take pro-active responsibility for monitoring their adherence to anti-money laundering regulations and internal anti-corruption policies, rather than relying on regulators to oversee and intervene when legislation has been breached and crimes have already been committed.[37] The Bank of Baroda's apparent wilful indifference to the Guptas' shady dealings (only closing their accounts very late in the day, after billions had already been laundered through them) is a shameful example of complicity in state

---

[35] *Money Laundering: the SARs Regime Consultation Paper*, Law Commission, Consultation Paper No 236, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/07/Anti-Money-Laundering-the-SARs-Regime-Consultation-paper.pdf

[36] *Improving the UK's response to economic crime*, National Economic Crime Centre, https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre

[37] *Economic Crime Plan 2019-22*, HM Government and UK Finance, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf

capture, corruption and criminality. The Bank of Baroda should in my view have been punished for its actions.

59. In order to encourage strict adherence to money laundering regulations and company procedures regarding the same, it is recommended that banks and professional enablers should face additional sanctions at both an organisational and an individual level, in addition to those already included in the current anti-money laundering legislation. On an organisational level, licenses should be immediately stripped from banks if they consistently fail to meet the anti-money laundering standards expected and licenses should be automatically suspended (pending investigation) if it is suspected that they have facilitated money laundering or corruption. This would act as a powerful deterrent. On an individual level, there should be the introduction of a 'senior manager's regime' whereby senior management is personally responsible for the failures of their company over money laundering and corruption. Punishments should include removal of permission to work for any regulated entity (such as a bank), fines and perhaps even prison time (for the most serious offences). This would encourage management to take a more active role in ensuring that their institution adopts and effects anti-money laundering policies and procedures.

Corporates

60. Aside from banks and professional enablers, corporate entities can also be responsible for fostering an environment that allows corruption to flourish by continuing to do business with corrupt individuals. This is particularly concerning in the state procurement sector (where taxpayers' money is at stake) and in certain industries that have historically proved susceptible to corruption. Corporate entities therefore need to contribute to the fight against crime by changing the way that they do business.

Extractive Industries Transparency Initiative (EITI)

61. Recommendation: Establishment of standards for good governance (based on the EITI standards) for industries that are vulnerable to corruption

62. EITI is a global standard for good governance of businesses operating in the mining, oil, gas and other extractive industries. It promotes greater transparency and accountability amongst the industry players through practical policies and procedures designed to combat money laundering and corruption. Those that adhere to the EITI standard publically disclose information from the point of extraction, right up to how the public is benefited. Government, companies and civil society are expected to collaborate and cooperate to promote understanding of resource management to prevent improper exploitation of resources. For example, EITI members are required to disclose information related to how the sector is managed so that there is an understanding of the laws and procedures for the award of production licenses. This information includes the process for awarding a license, information about the recipient of the license and any material deviations from the tender framework.[38] Disclosure of this level and type makes it difficult for licenses to be awarded outside of the established framework without attracting criticism and challenge from bidders and the public.

63. The extractive industries are not the only business areas that have been historically vulnerable to corruption. The international community is in the process of considering establishing EITI equivalents for other vulnerable business areas that could benefit

[38] *The EITI Standard 2019*, The global standard for the good governance of oil, gas and mineral resources, 17 June 2019, https://eiti.org/sites/default/files/documents/eiti_standard2019_a4_en.pdf

from increased transparency, such as state procurement contracts. The guidelines for the state procurement sector would likely include requiring states to publicly publish information about the tender process and the successful tender party so that it is more difficult for tenders to be awarded illegally to counterparties without the necessary capability. A level of visibility around the successful tender party would make it easier for the state and other third parties to better understand who they are doing business with and whether that person poses a financial crime risk (see *Part Two – Transparency of Ownership*).

64. It is recommended that South Africa joins the EITI initiative as a matter of priority to help to tackle corruption in the South African extractives industries (as the Commission will be aware, state capture involved the misappropriation of extractive industries, including the sale of the Optimum coal mine to the Guptas[39]). To the extent that the EITI principles are rolled out to other sectors, either by EITI or by any new body, South Africa should ensure that it adopts the principles for those additional business areas too.

Black Economic Empowerment (BEE)

65. Recommendation: Increased transparency around BEE contracts

66. It is a sad reality that increased protection is needed in order to ensure that the important and legitimate aims of the Black Economic Empowerment (BEE) programme are not undermined through corrupt manipulation by a few corrupt individuals (such as the Guptas) and their illegal 'rent seeking'. Unfortunately, in recent history, contracts with state-owned enterprises have been awarded to enterprises under the BEE initiative that do not have or intend to obtain the requisite capability to properly perform those contracts, nor intend to further the aims of the BEE movement. In that regard. Part 1 of this document identified Gupta businesses and those related to the Free State that were often claimed to be BEE's but which did not deliver on their promises or empower black communities. Therefore, special attention must be paid to better regulating and promoting the BEE programme (over and above the general state procurement recommendations set out immediately above) to ensure that it offers the intended benefits.

67. It is recommended that, in addition to the disclosure of information regarding BOs and contractual counterparties (see *Part Two – Transparency of Ownership* and *Information Sharing*), there must be increased transparency around whether BEE parties (i) have a relevant track record; (ii) meet basic up-skilling requirements to perform a contract e.g. do hire and train black employees to the number and qualifications required for competency under the contract; and (iii) satisfactorily perform their contract against contractual key performance indicators including final sign-off on completion. The number of employees retained by businesses claiming to operate as a BEE enterprise should also be recorded, verified and disclosed, as those that exploit the BEE initiative usually create a shell company with very few employees (much fewer than would be needed to fulfil the contract) solely to win the contract. In other words, they pervert the admirable and necessary objectives of BEE. This additional transparency could be achieved in the form of regular public updates by the state through the Department of Public Enterprises websites and a whistle-blowing hotline for the reporting of breaches

[39] *Clear signal to foreign investors: Hasty go ahead for Guptas to Buy Optimum*, Biz News, 23 February 2016, https://www.biznews.com/sa-investing/2016/02/23/clear-signal-to-foreign-investors-hasty-go-ahead-for-guptas-to-buy-optimum

68. Given that the BEE programme is so important to the future of South Africa and has been wrongly exploited and manipulated by state capture criminals over a protracted period, greater transparency and accountability in this area is essential to ensure that: (i) those whom the initiative was designed to benefit are able to benefit; (ii) the South African people are provided with the goods or services promised under a state contract; and (iii) financial institutions who bank BEE's, the press and local communities can identify rogue BEEs so that they cannot move any ill-gotten 'rents' abroad and out of easy reach.

States

69. States that wish to maintain or enhance their status as global financial centres or successful environments for business opportunities must bolster their commitment to tackling financial crime. Money laundering almost always involves the transfer of funds across borders, as criminals seek to exploit the complexity inherent in the global financial system and the differences between different state laws and regulations. Central to a state's ability to strengthen and enforce anti-money laundering legislation is whether its regulators have been suitably armed with the necessary powers and the requisite funding. Regulators should be able to investigate and punish all of those who commit serious financial crime. Closer bonds should also be established between states (and their regulators) to ensure that there is a stronger collective defence against criminals exploiting jurisdictions with weaker anti-money laundering legislation or more opaque financial systems.[40]

Legislation

70. Recommendation: (ii) proper utilisation of existing legislation; (ii) implementation of additional measures to hold public officials to account for misusing information gathered during an investigation; (iii) implementation of additional measures to recover the proceeds of crime (e.g. unexplained wealth orders); and (iv) additional funding for regulators

71. South Africa, along with many other states, has strong anti-money laundering and corruption legislation in place (such as the Prevention and Combating of Corrupt Activities Act 2004[41] and the Financial Intelligence Centre Act 2001[42]) that makes it an offence to engage in money laundering or other corrupt activities. However, this legislation was not suitably enforced to combat financial crime, allowing state capture to occur and third parties in other jurisdictions to facilitate financial crime. Therefore, the first priority of the South African government and other states must be to ensure that regulators are properly utilising the anti-money laundering legislation already in existence to hold criminals to account.

72. In applying anti-money laundering legislation, states should not be afraid to hold public officials to account. If anything, they should be held to a much higher standard of accountability than others given their role as elected officials acting on behalf of the South African people. It is recommended that the accountability of public officials is

---

[40] *Economic Crime Plan 2019-22*, HM Government and UK Finance, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf

[41] *Prevention and Combating of Corrupt Activities* (Act No. 12 of 2004), http://www.justice.gov.za/legislation/acts/2004-012.pdf

[42] *Financial Intelligence Centre Act*, 2001 (Act No. 38 of 2001), https://www.fic.gov.za/Documents/FIC%20Act%20with%202017%20amendments%20(1)%20(1).pdf

strengthened by introducing new anti-money laundering legislation in South Africa to hold public officials criminally liable for misusing information gathered during an anti-corruption investigation. Although such behaviour is criminalised in SA legislation, the fact that there has been no prosecution of the misuse of information has more to do with the "hollowing out"/dysfunctionality of SA law enforcement authorities as a result of state capture than it has to do with laws on the statue book. The people of South Africa have put their trust in their government officials and these individuals should not be allowed to prosper at their expense.

73. It is also recommended that South Africa introduces additional robust and dynamic tools to assist regulators with recovering the proceeds of crime more easily and to encourage regulators to monitor and investigate parties suspected of facilitating money laundering or corruption. South Africa must review the anti-corruption and anti-money laundering measures being adopted by other states, adopting any that it feels would assist its regulators to better hold criminals to account and recover the proceeds of crime. For example, the UK has recently introduced unexplained wealth orders (UWOs) into the UK regulators' toolbox. These orders require a person to explain the source of wealth used to acquire certain property in the UK. In the event that a legitimate explanation is not provided, the property is seized by the regulators and deemed recoverable proceeds of crime. This regulation allowed the UK's National Crime Agency to require the wife of a jailed banker (who was convicted of embezzling up to $3 billion in Azerbaijan) to explain how she had come to acquire certain valuable properties and assets in England worth over £22 million.[43]

74. Coupled with stronger enforcement powers is the need for a commitment to funding regulators. It is recognised that funding regulators can be politically difficult when there are a number of budgetary considerations and, ultimately, the level of funding will be influenced by the electorate and the political mandate of those in power. However, the less funding regulators receive, the less investigations will be conducted, the less funds recovered and the less criminals held to account. It is recommended that funding is increased for regulators, in particular South African regulators, to enable them to properly perform their function.

Financial Action Task Force (FATF)

75. Recommendation: Fully implement all of the FATF recommendations

76. States should strive for increased universality in anti-money laundering policies and procedures. This will ensure that the standard is raised in states where financial corruption is endemic (such as the United Arab Emirates, China and Hong Kong) and there is commonality across borders, reducing confusion as to what anti-money laundering standards apply in what country. Whilst it is imperative that each state passes its own laws legislating against money laundering, basing such legislation on the same set of principles would help ensure universality. The Financial Action Task Force (FATF) has proposed a set of recommendations aimed at preventing, detecting and sanctioning money laundering that should be adopted by all states and should underpin national legislation on this issue.

77. South Africa is a member of the FATF. However, simply being a member and agreeing with the recommendations is not sufficient. South Africa must actively implement the recommendations and ensure that national legislation reflects all of the recommendations. Furthermore, South Africa must monitor whether the

[43] *Azeri banker's high-spending wife targeted by new British anti-graft powers*, Reuters, 10 October 2018, https://uk.reuters.com/article/uk-britain-corruption-azerbaijan/azeri-bankers-high-spending-wife-targeted-by-new-british-anti-graft-powers-idUKKCN1MK1BR

recommendations are actively being applied. All law enforcement and regulatory authorities across South Africa must demonstrate their willingness to support the FATF standards, and thereby their commitment to eradicating corruption.

Mutual Legal Assistance

78. Recommendation: Increased mutual legal assistance

79. In order to prevent criminals evading justice by relocating themselves and their assets to another jurisdiction, states must develop closer bonds and work together to ensure that criminals are held to account wherever they are in the world. States should be prepared to "*rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering*"[44] and should do so expeditiously, before criminals are able to hide or disguise their ill-gotten gains. Based on the reported locations of the funds stolen laundered by the Guptas, fostering closer cooperation between South Africa and Hong Kong, the United Arab Emirates and India is of particular importance.

80. Mutual Legal Assistance Treaties (MLATs) offer a way of formally documenting cooperation between states to exchange information to assist in criminal investigations and hold criminals who have relocated themselves and their assets to another jurisdiction to account. MLATs can provide a state with access to information/assistance that could not normally be obtained through inter-law enforcement cooperation. In relation to financial crime specifically, the types of assistance that can be requested when an MLAT is in place include: (i) serving proceedings; (ii) obtaining special procedural material (e.g. records held by banks or accountants); (ii) search and seizure of evidence; and (iii) freezing or confiscation of assets.[45]

81. It is recommended that South Africa negotiate MLATs with other states where it is politically possible to formalise cooperation and to provide additional options to recover criminal property that has been moved overseas. It is further recommended that once signed, the process for formal ratification is completed within a three month period. For example, a MLAT (and extradition agreement) with Hong Kong was signed on 20 February 2009 but has yet to be submitted to parliament for ratification.[46] Where there are MLATs already in place, for example with India, better use must be made of those agreements to ensure that the proponents of financial crime are held to account.[47]

---

[44] *The FATF Recommendations*, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Adopted by the FATF Plenary in February 2012 and updated in June 2019, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[45] The UK's MLA guidelines provide a helpful overview of common requests received by the UK. See *Requests for Mutual Legal Assistance in Criminal Matters, Guidelines for Authorities Outside of the United Kingdom - 2015*, 12th Edition, The Home Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf

[46] *Extradition and Mutual Legal Assistance in criminal matters treaties*, Department of Justice and Constitutional Development, Republic of South Africa, http://www.justice.gov.za/ilr/mla.html

[47] *Extradition and Mutual Legal Assistance in criminal matters treaties*, Department of Justice and Constitutional Development, Republic of South Africa, http://www.justice.gov.za/ilr/mla.html

Extradition Agreements

82. Recommendation: Proliferation of responsible and effective extradition agreements

83. Extradition agreements, like MLATs, are another type of inter-state agreement that can be utilised to hold criminals to account and bring those who have fled overseas along with laundered funds to justice. States should "*constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay*"[48] to prevent those who have evaded justice from enjoying or hiding their ill-gotten gains or committing further offences. All governments must ensure that their country does not provide a safe haven for the perpetrators of state capture, looking to seek refuge beyond the reach of international justice (some of the main culprits being Dubai, Hong Kong and tax havens in the Caribbean). This requires the express criminalisation of money laundering and other types of financial crime as extraditable offences and agreements between states to extradite persons who commit those offences.

84. States must proactively engage with one another to ensure that criminals can be extradited quickly or risk the criminal relocating to another jurisdiction or dissipating the stolen funds. For example, whilst the extradition agreement and MLAT between South Africa and the United Arab Emirates is a positive step forward in bringing those responsible for the state's capture to justice, it has taken eight years of negotiations and the Guptas have yet to be extradited and are currently free to spend their billions, reducing any amount that will later be returned to South Africa.[49] Why? In my view, either the government under the Ruler of Dubai, Sheikh Mohammed bin Rashid Al Maktoum, is wilfully sheltering a family that has looted astronomical amounts from South African taxpayers, or the South African authorities do not have the capability/political will to insist that the Guptas are arrested and returned to South Africa to face trial.

85. It is recommended that South Africa negotiate extradition agreements with other states where it is politically possible to formalise cooperation and to provide a method for seeking the repatriation of criminals. It is, however, recognised that caution must be exercised in relation to states that do not observe the Universal Declaration of Human Rights in their justice systems. Where there are extradition agreements already in place, better use must be made of those agreements. Whilst a number of states are making good use of INTERPOL and Europol in pursuit of economic criminals, the effectiveness of any 'red notices' (i.e. international person wanted notice) issued is thwarted by the existence of extradition free havens for the perpetrators of corruption and financial crime.

86. Regardless of the existence of extradition agreements, states must be willing to cooperate and to cooperate expeditiously to ensure that criminals are held to account and it is suggested that ad-hoc agreements are reached with respect to specific individuals responsible for serious financial crime in the interim to speed the process up.

---

[48] *The FATF Recommendations*, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Adopted by the FATF Plenary in February 2012 and updated in June 2019, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[49] *Time up for the Guptas? Parliament approves extradition treaty with UAE*, news24, 15 November 2018, https://www.news24.com/SouthAfrica/News/time-up-for-the-guptas-parliament-approves-extradition-treaty-with-uae-20181115

CONCLUSION

87. In summary, my recommendations to the Commission are:

87.1. Increase transparency around the beneficial owners of corporates and strengthen the programme for auditing the due diligence conducted by banks and professional enablers to ensure that they are fully complying with anti-money laundering legislation and polices.

87.2. Increase the sharing of data within banks and professional enablers, between banks and professional enablers, and between banks, professional enablers and the state, so that there is greater visibility around the risk profile of customers and transactions.

87.3. Create additional penalties (at both an organisational level and an individual level) for banks and professional enablers who fail to self-police and act in accordance with anti-money laundering legislation and procedures.

87.4. Join the EITI so that there is greater transparency and accountability around the operation of the extractive industries; historically an area at higher risk of corruption.

87.5. Increase transparency around the BEE programme to ensure that the legitimate aims of this initiative are not subverted for the personal gain of criminals.

87.6. Ensure proper utilisation of anti-money laundering and corruption legislation in existence, as well as implementing additional legislation (to better hold public officials to account and to assist with recovery of assets) coupled with increased funding for regulators.

87.7. Fully implement all of the FATF Recommendations.

87.8. Increase mutual legal assistance between states.

87.9. Encourage extradition agreements between states.

Transparency and Fairness

88. Making the changes needed to combat financial crime, investigate potential corruption and repatriate stolen funds will not be easy. However, the people of South Africa deserve better than the obscene looting and devastation caused by state capture and I hope that the recommendations referenced in this report are also recommended by the Commission, and then implemented by the Government. South Africa has had, and still does, a corruption near death experience that must not be repeated and must be eradicated if the country is to survive and prosper in the future – and if the values of the freedom struggle are to be realised.

Lord Peter Hain House of Lords London SW1A 0PW
peter.hain@parliament.uk

PH-024

United Nations Office on Drugs and Crime

UNODC Everywhere

Money-Laundering and Globalization

Rapid developments in financial information, technology and communication allow money to move anywhere in the world with speed and ease. This makes the task of combating money-laundering more urgent than ever.

The deeper "dirty money" gets into the international banking system, the more difficult it is to identify its origin. Because of the clandestine nature of money-laundering, it is difficult to estimate the total amount of money that goes through the laundry cycle.

The estimated amount of money laundered globally in one year is 2 - 5% of global GDP, or $800 billion - $2 trillion in current US dollars. Though the margin between those figures is huge, even the lower estimate underlines the seriousness of the problem governments have pledged to address.

There have been a number of developments in the international financial system during recent decades that have made the three F's-finding, freezing and forfeiting of criminally derived income and assets-all the more difficult. These are the "dollarization" (i.e. the use of the United States dollar in transactions) of black markets, the general trend towards financial deregulation, the progress of the Euromarket and the proliferation of financial secrecy havens.

Fuelled by advances in technology and communications, the financial infrastructure has developed into a perpetually operating global system in which "megabyte money" (i.e. money in the form of symbols on computer screens) can move anywhere in the world with speed and ease.

For more information about other organizations involved in anti-money-laundering and countering the financing of terrorism (AML/CFT) activities, please see related links.

Copyright©2019 UNODC, All Rights Reserved,

PH-025

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-026

ANALYSIS

State Capture wipes out third of SA's R4.9-trillion GDP – never mind lost trust, confidence, opportunity

By Marianne Merten • 1 March 2019

Caption

Subscribe 116k

2737 Reactions

The cost of State Capture hovers at around R1.5-trillion over the second term of the Jacob Zuma administration. That's just short of the R1.8-trillion Budget for 2019. Put differently, State Capture has wiped out a third of South Africa's R4.9-trillion GDP, the country's total product, or effectively annihilated four months of all labour and productivity of all South Africans, from hawkers selling sweets outside schools to boardroom jockeys.

Overnight news and latest Daily Maverick features by 6am. Totally free

Your email

Signup here

Follow

Save

Listen to this article

18:44

AddThis (https://www.addthis.com/website-tools/overview?

PH-027

Quantifying the cost of State Capture is a Gordian knot. There are some costs that hit hard and immediately, although their final impact can be mitigated, at least to some extent, over time. Other costs creep on to the balance sheets of, for example, state-owned entities (SOEs) such as Eskom or government departments, where they look as if they belong as "finder's fees", "consultancies" and "commissions", but they don't, as these are effectively kickbacks.

The price tag of a culture of imperviousness for politically connected players, and a flailing governance system, can be obscured. And the impact of reputational damage, broken trust and loss of opportunities is hard, if not impossible, to fully quantify, regardless of the cleverest modelling system.

But there are some readily available numbers in the public domain.

This article belongs to our archives of over 30,000 pieces of work over the past decade.

You can access our entire archives with one of the following options:

Join Daily Maverick

Become a Maverick Insider (/insider/?referrer=jamatto&module=archive&return_url=https%3A%2F%2Fwww.dailymaverick.co.za%2Farticle%2F2019-03-01-state-capture-wipes-out-third-of-sas-r4-9-trillion-gdp-never-mind-lost-trust-confidence-opportunity%2F)

Sign in to Daily Maverick (it's free) (/sign-in/?referrer=jamatto&module=archive&return_url=https%3A%2F%2Fwww.dailymaverick.co.za%2Farticle%2F2019-03-01-state-capture-wipes-out-third-of-sas-r4-9-trillion-gdp-never-mind-lost-trust-confidence-opportunity%2F)

Support our archives directly

Day Pass **R4**

1 Month Pass **R60**

6 Month Pass **R300**

Restore purchase »

×

No thanks, I don't want to pay or register

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

And as US Senator Everett Dirkson, cautioning about out-of-control federal spending in his days, reportedly said:

"A billion here, a billion there, pretty soon you're talking real money."

South Africa's Budget lost R252.5-billion between 2007, when official data showed a R9.5-billion surplus in the national coffers (and expectations to have money in the kitty for the next three years), to today, when the 2019 Budget reflected a R246-billion hole that has to be plugged through borrowing and leaving less money for service delivery and governance.

AddThis (https://www.addthis.com/website-tools/overview?utm_source=AddThis%20Tools&utm_medium=image)

PH-028

utm_source=AddThis%20Tools&utm_medium=image)

Borrowing requirements shot up by some R67.1-billion in just four years from the R178.9-billion needed in 2015. For this reason, debt service costs are the biggest increasing Budget item: R202.2-billion in debt repayments in 2019, up from R147.7-billion debt service costs in 2016 — and escalating from an initial approximately R15-billion more from 2016 to 2017 to R20-billion more from 2018, according to the various Budget Reviews.

Economic growth plunged from 4.9% in 2006 to 2.3% in 2010, when Budget documents forecast an increase to 3.6% amid upbeat sentiment in the 2010 Budget Review that "the global storm has subsided and the South African economy is well on the path to recover[y]".

But by 2014, economic growth had plunged to 1.5%, down from 2.2% just a year earlier, and fell further to 1.3% in 2015 on a consistent downward slide — ending at 0.7% in 2018. If the current modest 1.9% growth for 2019 does not materialise, serious questions must be asked as to whether the state of South Africa's economy, and government's ability to deliver on a better life, are just the delusions of a political elite in search for votes.

R506-billion was wiped off the value of South African bonds and listed companies, where pension funds are heavily invested, after the midnight end-of-March 2017 Cabinet reshuffle that saw Pravin Gordhan and Mcebisi Jonas booted from the finance ministry.

That Cabinet reshuffle was widely seen as a firm attempt by Zuma to secure ministers favourably disposed to the Guptas and their businesses.

Then finance minister Malusi Gigaba never really shook off that Gupta tag, and two of the three international ratings agencies reacted bluntly: South Africa was downgraded to junk status by Fitch and Standard & Poor's in April 2017, both citing institutional and political uncertainty in the wake of the Cabinet reshuffle, policy uncertainty, and possible changes of direction with regard to nuclear power and SOEs.

Gordhan, now public enterprises minister, in November 2018 testified before the Zondo State Capture Commission about the cost of this reshuffle:

> "The devastating impact of this unexpected and [illegible] is estimated to be approximately R500-billion... Over two [illegible] the country's 17 biggest financial and property shares fell by R290-billion. The figure excludes the remainder of the equities market that also was hit by the decision. South African bonds lost 12% of their capital value (R216-billion)."

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

R378-billion had been wiped out on the Johannesburg Stock Exchange (JSE) and some 148,000 jobs (https://www.timeslive.co.za/politics/2018-11-23-zumas-sacking-of-nhlanhla-nene-cost-148000-jobs-zondo-inquiry-hears/) — in what is known as South Africa's 9/12, the evening Nhlanhla Nene was dismissed as finance minister in December 2015, in particular over his opposition to the R1-trillion nuclear deal that the Zuma administration was pushing.

AddThis (https://www.addthis.com/website-tools/overview?utm_source=AddThis%20Tools&utm_medium=image)

PH-029

utm_source=AddThis%20Tools&utm_medium=image)

Finance Director-General Dondo Mogajane, in a note to his testimony before the Zondo commission, clearly states debt service costs in the 2016 Budget were R5-billion higher than initially planned because of the impact of Nenegate, that pushed up South Africa's borrowing costs by one percentage point.

The costs of State Capture also arise in the drop of foreign direct investment (FDI). In 2017 FDI stood at $1.3-billion (about R18-billion), down from $4.5-billion (about R63-billion) in 2012, according to the United Nations Conference on Trade and Development (Unctad) 2018 World Investment Report (https://unctad.org/en/PublicationsLibrary/diaeiainf2019d1_en.pdf?user=46). And the report directly links politics and economics:

"FDI to South Africa declined by 41% to $1.3-billion, as the country was beset by an underperforming commodity sector and political uncertainty."

Add into the mix R200-billion overspent on Medupi and Kusile, according to a Public Enterprises briefing to MPs in February. Shoddy workmanship first discovered there in March 2013 — 9,000 welding faults in boilers, according to *Business Day* at the time — continues to this day in the deal forged in political connectivity that profited the ANC investment company Chancellor House to the tune of at least R50-million. It recently emerged that the Special Investigating Unit (SIU) is investigating theft and corruption of R139-billion at those two power stations, as *Fin24* (https://www.fin24.com/Economy/siu-probes-r139-billion-rot-at-medupi-and-kusile-report-20190224) reports (https://www.fin24.com/Economy/siu-probes-r139-billion-rot-at-medupi-and-kusile-report-20190224), part of its probe into misappropriations at Eskom amounting to R170-billion.

And then there is the R419-billion Eskom debt that makes the power utility the most significant risk to the South African economy. The debt has been incurred against government guarantees of R350-billion, and if Eskom defaults it sets in motion a complex cross-default call-in of debt that would cut across SOEs and also affect SAA, which has government guarantees of R19.1-billion.

Eskom's debt ballooned from R40.5-billion in 2007 to R254.8-billion in 2014, and R419-billion today amid consistently above-inflation tariff hikes. [illegible] events that the 2018 parliamentary Eskom State Capture [illegible] procurement deals and appointments of executives and board members.

State Capture costs must include the roughly R90-billion [illegible] collected tax revenue between 2015 and 2018 — a R48.2-billion shortfall in 2018, R30.4-billion in 2017 and R11.6-billion in Budget 2016. It's directly linked to the South African Revenue Service (SARS) unravelling in politically motivated State Capture machinations under ex-head Tom Moyane, a close Zuma ally from exile days in Mozambique. Officials do not deny taxpayer morality declined and more sought (legal) ways not to pay their dues, as is borne out in tax collection rates.

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

AddThis (https://www.addthis.com/website-tools/overview?

PH-030

utm_source=AddThis%20Tools&utm_medium=image)

In May 2018 MPs in Parliament's finance committee were bluntly told by the Tobacco Institute of South Africa (Tisa) that due to State Capture at SARS, South Africa lost R5-billion in custom and excise taxes during 2017 alone, or R27-billion since 2014.

Like the capture of SARS has had a direct impact on monies, but also institutional capacity, State Capture through the appointment of politically pliant officials has affected the prosecution service, the SAPS and the Hawks. Aside from internecine internal battles, the costs of State Capture mean actions that should have happened, didn't.

Or as South African Reserve Bank (SARB) Deputy Governor Kuben Pillay told MPs on the parliamentary finance committee as far back as August 2017, it was unclear what had happened to the 41 suspicious cases the SARB had referred for criminal investigation by the law enforcement agencies in the previous five years (http://www.dailymaverick.co.za/article/2017-08-02-reporters-parliamentary-diary-clear-uncertainties-or-we-remain-in-recession-says-sarbs-lesetja-kganyago/).

This is part of what could be called soft State Capture, where the impact is not so much measurable in rands and cents, but rather the impunity put on a show by politicians and the politically connected.

And so, former SAA board chairperson and executive director of the JG Zuma Foundation, Dudu Myeni, went head-to-head with at least two finance ministers in late 2015 over SAA aircraft deals that would have seen the cost of new aircraft balloon due to R603-million pre-payments to a middleman. Earlier in 2015 Myeni had called then Eskom board chairperson Zola Tsotsi to a meeting at then president Jacob Zuma's official Durban residence to discuss the power utility. Or, as Tsotsi told MPs (https://www.dailymaverick.co.za/article/2017-11-23-parliament-lynne-brown-ranges-between-attack-and-denial-in-bruising-six-hour-state-capture-interrogation/#.WuGyvGaBog4) in the parliamentary State Capture inquiry:

"Ms Myeni then proceeded to outline the purpose of the meeting, namely, that the situation of Eskom's financial stress and poor technical performance warrants that an inquiry into the company be instituted. She further elaborated that [illegible] executives, namely acting chief executive Tshedisa Matona, [illegible] capital Dan Marokane and group executive for commercial Matshela Koko, are to be suspended..."

Although MPs wanted to hear from Myeni, she claimed ill [illegible] invited in February 2018, and subsequently flouted a subpoena from Parliament to appear before the Eskom State Capture inquiry. The final report (https://www.parliament.gov.za/storage/app/media/Links/2018/November%202018/28-11-2018/Final%20Report%20-%20Eskom%20Inquiry%2028%20NOV.pdf) was adopted by the National Assembly in early December 2018, and is now, with supporting documents, witness statements and other documentation, with the Zondo Commission.

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

AddThis (https://www.addthis.com/website-tools/overview?

PH-031

utm_source=AddThis%20Tools&utm_medium=image)

But a culture of untouchability runs through government. In the reports Auditor-General Kimi Makwetu released in 2018, only 33 of South Africa's 257 councils had a clean bill of health, while at the national and provincial level, only 28% of departments had "no findings on compliance with legislation". For many consecutive years, Makwetu and his predecessor Terence Nombembe had the same refrain: Lack of compliance with prescripts and the law, lack of political will and lack of consequences for wrongdoing.

And so 14 councils invested R1.5-billion of monies they received for service delivery and other projects in VBS Mutual Bank in contravention of the law, the Municipal Finance Management Act (MFMA), and against a caution by National Treasury not to invest. And while, for example, Vhembe district ANC mayor Florence Radzilani (https://ewn.co.za/2019/02/19/former-vhembe-mayor-radzilani-out-to-clear-her-name-in-vbs-saga) resigned, insisting she had done nothing wrong, earlier news reports said she had complained about getting only R300,000 for Christmas from VBS.

All these 14 councils (https://www.dailymaverick.co.za/article/2018-05-31-dire-straits-for-municipalities-as-their-deposits-in-vbs-mutual-bank-may-be-unrecoverable/) are on the list of 87 dysfunctional councils identified in May 2018 by Co-operative Governance Minister Zweli Mkhize.

Water and Sanitation, which received a qualified audit in 2017 and clocked up R5-billion in irregular expenditure, paid invoices for engineering and project management hours that would have meant the consultant was working 24/7 at a rate well above what is stipulated by Public Services and Administration, Parliament's watchdog on public spending.

That emerged in a series of meetings in 2018 by the Standing Committee on Public Accounts (Scopa), which also heard there is still no access to safe drinking water for all villagers under the Giyani water project, despite costs ballooning to R2.2-billion in 2017, from R1.3-billion just a year earlier.

On Wednesday Parliament's environmental affairs committee in a statement welcomed that the project's trenches had now finally been closed — after the death of six-year-old Nsuku Baloyi, who fell into one such uncovered trench of this Giyani water project (https://[illegible]).

Meanwhile, in the Eastern Cape, investigations are underway into why a contractor was paid R4.8-million to replace nine pit toilets, when that was meant for 12 toilets and the renovation of several classrooms, according to *City Press* (https://city-press.[illegible].com/News/148m-for-nine-pit-toilets-heres-what-the-company-owner-has-to-say-20190218).

There are straightforward State Capture costs that have been in the public domain for at least three years, confirmed in the #GuptaLeaks. This includes the R1-billion Eskom paid to international consultants McKinsey, the R659-million coal prepayment for Gupta-owned Tegeta in April 2016 that effectively facilitated its acquisition of the Optimum coal mine, and the R5.3-

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

AddThis (https://www.addthis.com/website-tools/overview?

PH-032

utm_source=AddThis%20Tools&utm_medium=image)

billion finder's fee to a Gupta-linked company as part of the 1,064 new locomotive deal by Transnet (https://www.dailymaverick.co.za/article/2017-10-23-amabhungane-the-mckinsey-dossier-part-5-how-transnet-cash-stuffed-gupta-letterboxes/).

McKinsey repaid the R1-billion some eight months after London-based McKinsey senior partner David Fine told the parliamentary Eskom State Capture inquiry in mid-November 2017 that the consultancy "did not want any tainted money. Our understanding is we went into a relationship with Eskom in good faith… They gave us verbal commitment they had National Treasury approval (https://www.dailymaverick.co.za/article/2017-11-16-parliament-lynne-browns-background-machinations-to-the-state-capture-inquiry-exposed/)".

Civil proceedings have been underway since January 2019 to recover at least R1.3-billion from former executives, according to Transnet board chairperson Pogo Molefe, as *Fin24* (https://www.fin24.com/Companies/Industrial/just-in-transnet-issues-summons-to-top-former-execs-20190117) quotes him saying: "One would not be exaggerating to say what we found there (at Transnet) was a horror show."

Molefe is part of the crop of new board members and executives appointed to troubled SOEs since early 2018. At Eskom, this meant that scrutiny of the books uncovered further irregular spending: it rose to R19.6-billion in 2018 from R5-billion just a year earlier. And while irregular expenditure does not necessarily mean corruption, or losses, it does mean procurement and other processes were not properly followed and requires each instance be investigated, according to the Public Finance Management Act.

To date, it's unclear whether, or what, steps are being taken to recoup the R659-million spent on the Tegeta deal that was described in the parliamentary Eskom State Capture inquiry report as part of a series of "questionable" decisions taken by a new board appointed under then public enterprises minister Lynne Brown.

"The Board oversaw some questionable procurement decisions, including the resolution taken on 9 December 2015 regarding an unprecedented prepayment to Tegeta ahead of its acquisition of (Optimum)…"

The Stellenbosch-based Bureau of Economic Research (BER) in October 2018 calculated that South Africa's GDP could have been anything between 10% and 30% higher, and between 500,000 to 2.5-million more jobs could have been created by 2017, according to the *Financial Mail* (https://www.timeslive.co.za/politics/2018-10-12-r1-trillion-the-cost-of-the-zuma-years/). And between R500-billion to R1-trillion more tax revenue could have been collected over 2010 to 2017. Or as BER economist Harri Kemp is quoted:

"If domestic post-crisis growth had matched that of SA's peers, citizens and the government would have been in a much better position than is now the case."

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

AddThis (https://www.addthis.com/website-tools/overview?

PH-033

utm_source=AddThis%20Tools&utm_medium=image)

State Capture has extracted an enormous price directly and indirectly on South Africans, most harshly on the poorest and most vulnerable, who cannot opt for private housing, private health insurance, private education and private security.

Here's how the cost of State Capture adds up to R1,5-trillion over the past four years or so:

- R252,5-billion in lost Budget,
- R67-billion more in debt service costs,
- R90-billion lost in tax revenue collection.
- R506 billion were lost from the value of South African bonds and listed companies in the March 2017 midnight Cabinet reshuffle,
- Nenegate wiped out R378-billion from the JSE.
- R200-billion overspent on Medupi and Kusile coal power stations that are not only over budget but also overdue in completion.
- The directly State Capture identified costs include R1-billion McKinsey consultancy fee, R659-million Eskom prepayment for coal to the Gupta-owned Tegeta and the R5,3-billion finders fee to a Gupta-linked company in the Transnet locomotive deal.

There are other costs arising from a plummeting economic growth rate, down to 0.7% in 2018 from 2,3% in 2019 and 2,2% in 2013 negatively impacting job creation and tax collection. And costs arise also from a culture of impunity within the government that allows service delivery project costs to balloon without completion while 4 councils invest R1,5-billion against the law in VBS Mutual Bank, instead of service delivery projects.

These calculations on the State Capture price tag don't even touch on the untold costs of loss of trust, reputation and opportunity. **DM**

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

AddThis (https://www.addthis.com/website-tools/overview?

PH-034

In other news...

"Richard Poplak is a rather contrived writer and a useless analyst. I mean, really, he clearly has never ever seen what the party has been through in the past... If you had to compare what Richard Poplak has done for democracy in South Africa compared to what many, many people have done including myself, it would pale into insignificance. I mean Poplak, who is Poplak? What kind of analytical background has he got?"
Helen Zille, Carte Blanche, 3 November 2019

Dear Helen

Richard Poplak, since you ask, is Editor-at-Large for Daily Maverick. He is also a contributor to the Financial Times, Atlantic Monthly, The Guardian, The National Post and the Globe and Mail. He regularly appears as a political commentator for Al Jazeera and the BBC amongst others as one of the most respected (and colourful) voices on South African politics.

He also happens to be South Africa's greatest wordsmith, sort of our own Hunter S Thompson, but with facts. And that's what makes him so deadly – so much so that you cannot contain your hatred for Poplak and for what he represents – a team of deeply competent journalists that cannot be bought, intimidated or fooled.

He's the recipient of the Bookmark Award for the best digital journalist in South Africa, a former Rockefeller Fellow and is a contributor to the global investigative collective – Deca stories.

Poplak was an integral member of the #GuptaLeaks team– arguably one of the biggest stories of political corruption anywhere on the planet, with our friends from amaBhungane and News24. The #GuptaLeaks team won the Taco Kuiper Investigative award, the Vodacom Journalist of the Year award and was cited for a Nat Nakasa 'Bravery in Journalism' award. Oh, and they have just won the most prestigious award in the world for investigative journalism: The Global Shining Light Award, 2019.

Helen, Richard Poplak was part of the team that broke #GuptaLeaks. You broke the DA.

These days, Daily Maverick is hated by Ace Magashule, Julius Malema and Helen Zille. We must be doing something right? That may sound facetious but the reality is we're not here to make friends with politicians. We exist to hold them to account and Defend Truth.

Help support us by becoming a Maverick Insider so that we can continue to expose corruption, bad governance and plain old incompetence. 'Cause if We don't... Who will? **For whatever amount you choose** , you can support DM and it only takes a minute.

Support Daily Maverick→

VISA MasterCard EFT

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

cost of State Capture (https://www.dailymaverick.co.za/article_tag/cost-of-state-capture/)

parliamentary State Capture inquiry (https://www.dailymaverick.co.za/article_tag/parliamentary-state-capture-inquiry/)

State capture (https://www.dailymaverick.co.za/article_tag/state-capture/)

Zondo commission of inquiry (https://www.dailymaverick.co.za/article_tag/zondo-commission-of-inquiry/)

AddThis (https://www.addthis.com/website-tools/overview?

PH-035

Marianne Merten

Follow | Save | More (https://www.dailymaverick.co.za/author/mariannemerten/)

Comments - share your knowledge and experience

Please note you must be a Maverick Insider (/insider/?utm_source=DM_Website&utm_medium=Comments) to comment. Sign up here (/insider/?utm_source=DM_Website&utm_medium=Comments) or sign in if you are already an Insider.

Comments

Comments are currently closed on this article. Articles are open for comment for one week after the date of publication.

ONLY MAVERICK INSIDERS CAN COMMENT. BECOME AN INSIDER

All Comments 10

HANNES JANSEN 8 months ago

Can some one please put together a 'photo' of what a MILLION rand in R100 notes will look like Better even if we could make up a pack of R100 notes equalling R1m and take it PARLEMENT so that they can get some comprehension of a Million ….even a Trillion.I do not think Parlement is big enough to house a trillion rand

HANNES JANSEN 8 months ago

It must be clear to one and all that the ANC Government and it's BEE strategy has failed SA tHE anc CAUCUS had 8 opportunities to remove JACOB ZUMA in votes of no confidence , they failed to act , and that makes them as culpable as JZ himself. BEE has only brought misery to SA - The skills level for an advanced and developed country is not their ...not even after 25 years of UHURU.The failing municipalities throughout SA is proof of this .So I guess if the majority of SA citizens wants to vote ANC they must take what is comingIF YOU LIVE BY THE SWORD YOU WILL DIE BY THE SWORD.....all in the name of BEE

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

Karsten Dopke 8 months ago

I feel ill...

Matthew Green 8 months ago

The questions is, "Okay, now what? What happens next?" Here we have some proverbial black and white information detailing what we already knew, if not quite to this extent. Thank you, Marianne Merten.When will those involved, complicit and otherwise be brought to account. If I skip a monthly repayment or two I am held to account. If my tax return is not submitted in a timely manner penalties and interest begins to accrue. What happens when my actions directly and indirectly have a negative affect on the lives of the people I have sworn to uphold and protect. Yes, I am

AddThis (https://www.addthis.com/website-tools/overview?...)

PH-036

directly and indirectly have a negative affect on the lives of the people of this country. Yes, I am looking at you Mr Zuma and all the other people fingered in this dastardly deed.

Colleen Dardagan 8 months ago

Marianne Merten thank you for this comprehensive piece, although I am not sure whether to cut my wrists or go and live under a tree somewhere and pretend this isn't all happening!! Your research and comprehensive coverage of this tragedy is exemplary. - Thank you!

Michael Hennessy 8 months ago

This is my problem with Zondo, Nugent et al. The commissions of enquiry are all well and good but all they do is fill you with horror and disgust. Satisfaction can only come when someone goes to jail. When is Kulubesi Zuma going to jail for Grootvlei? When is Duduzeni Zuma going to jail for culpable homicide for killing a taxi passenger with his fancyass Porsche? When is Dudu Myeni going to jail for money extorted from SAA? What about Brian Molefe and Optimum? When is ... Oh, just give up. The situation is irretrievable, we are doomed unto the second generation

Francoise Phillips 8 months ago

The headline should really read: The ANC wipes out a third of SA's GDP. Let's start calling a spade a spade. State Capture IS the ANC.

> **Tim Bester** 8 months ago
>
> ...and the comrades' strategy to achieve 'capture' is all written down in their NDR, for all to see.

> **Geoff Coles** 8 months ago
>
> That's it in a nutshell!.... We need arrests and charges now with dates arranged for quite a few of the Comrades for trial.... Too early to actually go to trail I suppose, but those charged, take away their passports.... those that aren't already gone!

Dbaileysa 8 months ago

Okay, so now we know what Zuma and his cronies cost the tax payer 1.8 trillion. How much of that is recoverable from the perps or is the damage done and we must all shut our faces and move on? With the NPA in the dwane and public-policing now non-existent any chance of success will be rate as what - minus 1.8 trillion? In other words, is there any good news for the uncorrupted tax payer other than cough up? Not even prison for a coupla years for JZ?

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

Related

BRIDGETTE vs BOTSWANA:

Springbok Rugby: Boks' Welsh wizard

AddThis (https://www.addthis.com/website-tools/overview?

PH-037

Bridgette Motsepe-Radebe attempts a Botswana explanation (https://www.dailymaverick.co.za/article/2019-11-01-bridgette-motsepe-radebe-attempts-a-botswana-explanation)

laid a foundation for RWC glory (https://www.dailymaverick.co.za/article/2019-11-12-boks-welsh-wizard-laid-a-foundation-for-rwc-glory)

BUSINESS MAVERICK: Obituary: Allan Gray: Death of a gentleman (https://www.dailymaverick.co.za/article/2019-11-12-allan-gray-death-of-a-gentleman)

Rugby World Cup 2019: The forgotten eight should never be forgotten (https://www.dailymaverick.co.za/article/2019-10-31-the-forgotten-eight-should-never-be-forgotten)

OP-ED: MEA CULPA: I was fooled by Iqbal Survé (https://www.dailymaverick.co.za/article/2019-11-07-i-was-fooled-by-iqbal-survé)

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

OPINIONISTA: Fearless leaders needed to offset the damage the demagogues are sowing now

AddThis (https://www.addthis.com/website-tools/overview?

PH-038

(https://www.dailymaverick.co.za/opinionista/2019-11-06-fearless-leaders-needed-to-offset-the-damage-the-demagogues-are-sowing-now)

utm_source=AddThis%20Tools&utm_medium=image)

EngageYa
(//www.engageya.com)

DAILY MAVERICK

ANALYSIS

Ayanda Dlodlo and the spies who don't love her – and our country

By Stephen Grootes

(https://www.dailymaverick.co.za/article/2019-11-13-ayanda-dlodlo-and-the-spies-who-dont-love-her-and-our-country/?utm_source=homepagify)

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

QUICK SEARCH AFRICAN NATIONAL CONGRESS (HTTPS://WWW.DAILYMAVERICK.CO.ZA/ARTICLE_TAG/AFRICAN-NATIONAL-CONGRESS/)
PUBLIC PROTECTOR (HTTPS://WWW.DAILYMAVERICK.CO.ZA/ARTICLE_TAG/PUBLIC-PROTECTOR/)
ZONDO COMMISSION (HTTPS://WWW.DAILYMAVERICK.CO.ZA/ARTICLE_TAG/ZONDO-COMMISSION/)
JACOB ZUMA (HTTPS://WWW.DAILYMAVERICK.CO.ZA/ARTICLE_TAG/JACOB-ZUMA/)
CYRIL RAMAPHOSA (HTTPS://WWW.DAILYMAVERICK.CO.ZA/ARTICLE_TAG/CYRIL-RAMAPHOSA/)
JULIUS MALEMA (HTTPS://WWW.DAILYMAVERICK.CO.ZA/ARTICLE_TAG/JULIUS-MALEMA/)

KZN TORNADO

(https://www.dailymaverick.co.za/article/2019-11-13-scores-injured-houses-destroyed-in-pietermaritzburg-tornado/?

PH-039

utm_source=AddThis%20Tools&utm_medium=image)
utm_source=homepagify)

Scores injured, houses destroyed in Pietermaritzburg tornado

Desiree Erasmus 7 hours ago

(https://www.dailymaverick.co.za/cartoon/party-poopers/?utm_source=homepagify)

ZAPIRO

Party Poopers

Zapiro 17 hours ago

(https://www.dailymaverick.co.za/section/newsdeck/?utm_source=homepagify)

NEWSDECK

News and reports from around

Last updated: 4 hours ago

DISPLAY ADVERTS ON OFF

OPINIONISTA

Government doesn't seem to grasp the meaning of SA's parlous finances
(https://www.dailymaverick.co.za/opinionista/2019-11-13-government-doesnt-seem-to-grasp-the-meaning-of-sas-parlous-finances/?utm_source=homepagify)

Nazmeera Moola • 8 hours ago

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

(https://www.dailymaverick.co.za/opinionista/2019-11-13-government-doesnt-seem-to-grasp-the-meaning-of-sas-parlous-finances/?utm_source=homepagify)

AddThis (https://www.addthis.com/website-tools/overview?

PH-040

Flying the American flag upside down is an officially recognized signal of distress. As is posting photos on this publication.

MAVERICK CITIZEN: PHOTO ESSAY

Springbok Champions Tour: Tribute to the Cape Town fans

Tevya Shapiro and Anso Thom • 7 hours ago

(https://www.dailymaverick.co.za/article/2019-11-13-springbok-champions-tour-tribute-to-the-cape-town-fans/?utm_source=homepagify)

OPINIONISTA

We can't just keep getting

Mark Barnes

(https://www.dailymaverick.co.za/opinionista/2019-11-13-we-cant-just-keep-getting-older/?utm_source=homepagify)

8 hours ago

MAVERICK CITIZEN

Madonsela: Reviews of administrative laws need ubuntu

Carmel Rickard

(https://www.dailymaverick.co.za/article/2019-11-13-madonsela-reviews-of-administrative-laws-need-ubuntu/?utm_source=homepagify)

9 hours ago

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

WESTERN CAPE

How will you keep our children safe,

Sue Payne

(https://www.dailymaverick.co.za/article/2019-11-13-how-will-you-keep-our-children-safe-ebies-river-residents-ask-premier-winde/?utm_source=homepagify)

7 hours ago

OP-ED

South Africa needs

(https://www.dailymaverick.co.za/article/2019-11-13-south-africa-needs-better-politicians-or-smarter-political-alliances/?utm_source=homepagify)

AddThis (https://www.addthis.com/website-tools/overview?

PH-041

utm_source=AddThis%20Tools&utm_medium=image)

better politicians

Ismail Lagardien

7 hours ago

LOAD MORE

×

Overnight news and latest Daily Maverick features by 6am. Totally free.

Your email

Signup here

AddThis (https://www.addthis.com/website-tools/overview?

4.30 pm

Lord Hain (Lab)

Share

My Lords, it is a real privilege to follow the noble Baroness. I have been in the House for less than two years, but she has always struck me as a real star. I have marvelled at the way in which she has managed to make the Government's case on Europe vaguely plausible, which shows expertise and charm. I have also noticed that the noble Baroness has always spoken and answered questions from the Front Bench, including from myself, with great courtesy, even giving the impression in her answers that she has listened to the questions. Her colleagues may well want to bear that in mind. I note that the casualty rate in the post that she has just left seems to be quite high. I wish her all the best in the future, and I am sure that the whole House does as well.

The noble Baroness made the case for sanctions against South Sudan and elsewhere compellingly. I do not refer to her specifically, but I remember the way in which this House opposed sanctions against the apartheid regime. If she had been in the Conservative Government at the time, perhaps that might have changed.

There have been no criminal prosecutions for money laundering of financial institutions, and very few of other "enablers" such as lawyers and accountants. There have been regulatory fines, but it is not clear that these are enough to deter banks and other financial players from making their anti-money laundering compliance regimes a tick-box exercise rather than a meaningful one. This Sanctions and Anti-Money Laundering Bill enables the Government to introduce regulations that would create new civil penalties and criminal offences for money laundering, but the threshold for the latter is low—a maximum three-month sentence for a criminal conviction.

As the noble Baroness, Lady Bowles, mentioned, using such powers to enable the Government to introduce criminal offences by regulation is against parliamentary convention. The noble and learned Lord, Lord Hope, also referred to this matter with his expertise. Surely it would be better for the Government to accept or introduce an amendment to the Bill

to introduce a “failure to prevent” money laundering offence, like that in the Bribery Act and as there now is for tax evasion, which would ensure that such an offence was introduced by primary legislation.

As I said, the noble Baroness, Lady Anelay, made moving points about South Sudan and elsewhere from her experience. However, my main focus today is whether the Bill will deal effectively with the massive money laundering organised from the very top of the Government in South Africa, the presidency itself—the subject of my Oral Question on 19 October in your Lordships’ House and my letter to the Chancellor of 25 September. I beg some indulgence in speaking at greater length than the noble Baroness on this to spell it out. It is serious.

Corruption within and money laundering from a monopoly capital elite around the President’s family in South Africa and their close associates the Gupta brothers—which is painful for me to witness, having been active along with my brave parents in the anti-apartheid struggle—show that winning the war against financial crime will require co-ordination, influence, action and accountability between multi-jurisdictional law enforcement agencies. Money laundering is a key enabler of organised crime, allowing criminals to transmit multi-billion pound illicit funds into the legitimate economy, undermining its integrity and public trust. However, confronting it is difficult, partly due to the fragmented information-sharing arrangements across borders and between banks and law enforcement agencies. It is all very well to develop better protection for our own country, as this Bill purports to do, but, without simultaneously enhancing cross-border co-operation, we will not win the war against financial crime.

On regular visits to South Africa—most recently last month—I have been stunned by the systemic transnational financial crime network facilitated by an Indian-South African family, the Guptas, and the presidential family, the Zumas. If there had been more proactive and genuine co-operation between the multi-jurisdictional law enforcement agencies, and within and between the banks, which have been moving money for the Gupta/Zuma laundering network, the devastation wrought on South Africa could have been significantly reduced, and

perhaps the financial institutions involved would have been able to better mitigate their exposure.

I had delivered by hand last night to the Chancellor printouts of transactions and named the British bank concerned, and I asked that he again refer these to the Serious Fraud Office, the National Crime Agency and the Financial Conduct Authority for investigation. This information shows illegal transfers of funds from South Africa made by the Gupta family over the last few years from their South African accounts to accounts held in Dubai and Hong Kong. The last columns of each sheet, now in the Treasury, show the relevant banks involved, and the records show all account numbers used. Many of the transactions are legitimate, but many certainly are not.

The latter illicit transactions were flagged internally in the bank concerned as suspicious, but I am reliably informed that it was told by the UK headquarters to ignore it. That is an iniquitous breach of legal banking practice in the UK, which I trust Ministers would never countenance, and it is also an incitement to money laundering, which has self-evidently occurred in this case, sanctioned by a British bank, as part of the flagrant robbery from South African taxpayers of many millions of pounds and many billions of their local currency, the rand.

Each originating transaction would start with one bank account and then be split into a number of accounts a couple of times to disguise the origin. Undoubtedly, hard questions will need to be asked of the facilitating banks, because they have aided and abetted the Gupta money laundering activities. Can the Chancellor please ensure that such evident money laundering and illegality is not tolerated and that the bank is investigated for possible criminal complicity in this matter? Urgent action is needed to close down this network of corruption.

Then let us consider an example of the devastation caused to South Africa by cross-border money laundering. The Free State, one of nine provinces in the country, is marked by miles of flat, rolling grassland and crop fields, and it is the country's granary, responsible for 70% of total maize production. Britain played a defining part in the history of this province, as it marked one of the most contested spaces during the late 19th century/early 20th century

South African wars involving the British imperialists, the Afrikaner nationalists and the Basotho people.

Today, the Free State is one of the poorest provinces in South Africa. Nearly one in two of the people are unemployed and nearly two-thirds live below what is called the "upper bound poverty line". More than half of the people in that province survive on one meal a day, tens of thousands of children go to school hungry, if they are fortunate enough to be in school, and over half of the province's children drop out of school before obtaining their matric—roughly equivalent to our A-levels—primarily because their daily focus is on survival.

Therefore, when in February 2013 the Free State Government announced that they would spend £18 million —approximately 340 million South African rand —to build, in a small Free State town called Vrede, a dairy farm which would be part-owned by 80 impoverished beneficiaries, the local community felt a sense of hope. Indeed, this kind of public/private partnership is a commendable and deeply necessary model of economic empowerment to redress the profound racial inequalities generated by the apartheid state, which continue to reverberate throughout South Africa.

What the people of Vrede did not know was that this project, and therefore their village, would become the scene of a transnational money laundering crime committed by collaborators from within the Free State Government on the one side and the now notorious Guptas on the other. In essence, this criminal network used these 80 people and their families as pawns in a swirl of international money laundering, which involved some British and other financial institutions.

The laundering operation went like this. Step 1: in May 2013, three months after the Free State Government announced the dairy farm project, a company called Estina—ostensibly the vehicle for the 80 beneficiaries but which was actually linked to the Guptas—was handed a farm to begin building the dairy. Estina's sole director was an IT salesman with no farming experience. The project was not put out to public tender. Step 2: the Government almost immediately transferred about £6 million to Estina. Step 3: instead of investing this in the farm, Estina transferred most of the money to a Gupta company in the United Arab Emirates called Gateway Ltd. Gateway is registered in Ras al-Khaimah, RAK, which is one of seven

emirates making up the UAE and a highly secretive offshore company jurisdiction. At the time, Gateway held its account with the British bank Standard Chartered, which the bank has subsequently closed.

Step 4: once the funds were in Dubai, the Guptas engaged in a classic laundering cycle, transforming illicit money into ostensibly legitimate assets. In arguably the most eye-watering example, they transferred over £2 million of the Estina dairy money in two separate tranches through two shell companies, ultimately consolidating it in their Standard Chartered account for another of their UAE-based companies, called Accurate Investments. The bank has since closed this account too. Step 5: they then transmitted this money into an entity called Linkway Trading, banked with the State Bank of India, back into South Africa.

Step 6: once in Linkway, the Guptas used these funds to pay for a lavish four-day family wedding where, among other extravagances, over £1,000 was spent on chocolate truffles, £120,000 on scarves for guests and £20,000 on fireworks. At about the same time that the Guptas were celebrating at the wedding, veterinarians in the town of Vrede were called to the dairy farm because of the reeking stench of dead animals. According to their report, they found at least 30 cows that had been buried in a ditch having died from,

"an unknown condition that could be caused by malnutrition".

I have detailed the Vrede dairy example because many of us do not appreciate the destitution caused by money laundering. It almost always requires the complicity, whether witting or unwitting, of financial institutions. In this case, some of those are headquartered in Britain, such as Standard Chartered. I am grateful that the bank is now being investigated, along with HSBC and the Bank of Baroda, by the Serious Fraud Office, the Financial Conduct Authority and the National Crimes Agency following my Question in your Lordships' House on 19 October and my request to the Chancellor.

The success of these criminal networks relies also on the action or inaction and co-operation or non-cooperation of the relevant law enforcement authorities. Always, it is the poorest who bear the brunt. In my letter to the Chancellor on 25 September requesting that he investigate UK bank exposure to the Gupta/Zuma network, I listed the 27 entities and individuals who

were, among others, involved in the Vrede dairy farm tragedy. It is by no means the only example of the devastation wrought on South Africa by the Zuma/Gupta network.

The Vrede dairy criminal catastrophe proves that the laundering was effected through a transnational triangulation between South Africa, the UAE and British and other global banks. Therefore, the success of our law enforcement authorities in protecting our country from the proceeds of ill-gotten gains entering our financial system, as this Bill seeks to do, and by association protecting more vulnerable developing nations from falling victim to extractive criminal networks, depends on genuine and proactive co-operation and collaboration between the relevant law enforcement agencies in the concerned jurisdictions. Frankly, this Bill falls well short of what is required to do that.

Familiarising myself with the Vrede dairy farm tragedy—and taking some time in this House to explain it—what struck me time and again is why an internationally respected bank such as Standard Chartered would open bank accounts for shell entities registered in a free trade zone such as Ras al-Khaimah, whose primary attraction is as a highly secretive offshore jurisdiction. What was it doing this for? Shell companies, by virtue of their ownership anonymity, such as those used by the Guptas in the Vrede dairy tragedy, are generally classic vehicles for money laundering and other illicit financial activity. According to the Financial Crimes Enforcement Network, shell companies,

“typically have no physical presence other than a mailing address, employ no one, and produce little to no independent economic value”.

The Financial Action Task Force, established in July 1989 at the G7 Paris summit, has consistently warned that free zones could be used for illicit trade and money flows that fall below the radar of regulatory authorities. We know that free zones have become an increasingly popular mechanism for the UAE and other countries looking to lure international investment and boost foreign trade. However, the question for us is whether we are ensuring that our financial institutions are facilitating, inadvertently or not, the misuse by those interests attempting to move their illicit funds from one part of the world to another in order to facilitate money laundering, mafia crime, terrorist activity and financing, as the Minister said, and robbery from taxpayers, as in the South African case.

There are disturbing questions around both the complicity, witting or unwitting, of UK global financial institutions in the Gupta/Zuma transnational criminal network, and also about these institutions' wilful blindness to the reality that the laundering process most often necessitates financial systems with lax regulation and controls. Unless we urgently find ways to leverage our respective capabilities to co-ordinate and influence action between the law enforcement and banking sectors—domestically here in the UK and globally—we cannot win this battle.

I have received new information, which is still being corroborated, that the Gupta/Zuma network may be using the global metal recycling sector—some of the company names I have received have a UK presence—to launder the proceeds of their corruption. Indeed, this preliminary information suggests that, as South African banks, including British headquartered ones there, have shut down Gupta accounts in response to the financial crime risk they pose, so the family has simply shifted its laundering machine into the metal recycling sector, using intermediaries within these companies in South Africa, the Middle East, possibly the UK and Hong Kong, to move their funds for them.

My question, therefore, to British-based financial institutions and to the Government is: are their compliance departments applying the necessary forensic eye to this secondary-layer threat—as primary accounts are shutdown, so the illicit funds must find alternative channels—and are law enforcement agencies and their regulators applying their minds, sharing information and, in so far as they can, acting on it?

My latest information, supplied as before by South African whistleblowers deep inside the system and disgusted by the corruption at the heart of the state, suggests metal recycling is the latest conduit. However, there may be other sectors these criminal networks are penetrating and I ask the Minister to investigate this.

Unless we use the opportunity before us to crack down meaningfully on these criminals, they will always be one step ahead. Over the past few months, several multinational companies have either fallen or been massively contaminated as a result of their complicity in the Gupta scandal, including Bell Pottinger, McKinsey, KPMG and SAP. The US Justice Department and the US Securities and Exchange Commission are now investigating German multinational SAP after it apologised the other week—"wholeheartedly and unreservedly"—

to the people of South Africa for paying over £6 million in kick-backs to Gupta companies as part of their network of corruption headed by President Zuma and his family.

I believe that it is a matter of time before financial institutions in South Africa, in the Middle East, in Hong Kong, here in the UK and in the US will be forced to answer hard questions about their own complicity, and they must. I am today sending a copy of this speech, together with my letter of 25 September to the Chancellor, to the US Ambassador to London formally asking the US regulatory authorities to intervene, as the FBI has already begun to do. I am also asking the Government—I would be grateful if the Minister could respond on this point—to press the financial authorities in Hong Kong and Dubai to cut all links with the Guptas and Zumas. My Labour MEP colleague Neena Gill is raising the matter in the European Parliament, and Commissioner Pierre Moscovici has agreed to her request to investigate European banks which may be involved. In parallel, I wrote to the President of the European Commission, Jean-Claude Juncker, on 25 September asking him to act, but have not yet had a reply.

It is not only financial institutions and Governments which need to ensure that they are above reproach. A number of other global firms, whether legal, auditing, forensic or advisory in nature, have provided professional services to some of these complicit individuals, companies and institutions. These include UK-based firms such as Grant Thornton and Hogan Lovells, which have conducted forensic investigations at the South African Revenue Service under the brief of its Gupta-aligned head, Tom Moyane. Norton Rose Fulbright and Morrison & Foerster have assisted in the internal investigation at McKinsey into that company's links to the Guptas. There are other examples. I am not suggesting that these firms are necessarily complicit in the corruption, because in most cases they have been employed by the complicit companies—for example, Norton Rose and Morrison & Foerster by McKinsey—to try and surface the corruption.

In conclusion, I am suggesting that it is absolutely critical that all professional firms cut their contacts entirely with any individuals or entities associated with the Gupta and Zuma families or their associates. At the very least, whatever pressure they may come under from their clients and whatever the cost is to their commission or fees, they must conduct themselves

according to the highest professional standards, which most if not all have palpably failed to do so far, as we saw with KPMG, McKinsey and SAP. To its credit, the law firm Cliffe Dekker Hofmeyr recently upheld the highest professional values by boldly exposing corruption and dishonesty by senior executives at the country's power utility, Eskom.

As I stand here today, the 80 individuals who were supposed to benefit from the Vrede dairy farm are destitute. The complicity of our financial institutions in this, as well as the responsibility of law enforcers and regulators in all the concerned jurisdictions, should make UK Government Ministers and UK parliamentarians hang their heads in shame. Just as they were complicit in sustaining apartheid, so today they are complicit in sustaining the corrupt power elite in South Africa which is now betraying the legacy of Nelson Mandela and the anti-apartheid struggle.

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-051

India's Bank of Baroda Played a Key Role in South Africa's Gupta Scandal

- Published: Tuesday, 27 February 2018 09:13
- Written by Khadija Sharife (OCCRP) and Josy Joseph (The Hindu)

Tweet Share

India's state-owned Bank of Baroda -- one of the country's largest -- played a crucial role in the financial machinations of South Africa's politically influential Gupta family, allowing them to move hundreds of millions of dollars originating in alleged dirty deals into offshore accounts, an investigation by the Organized Crime and Corruption Project (OCCRP) and The Hindu has found.

PH-052

A man walks past the Bank of Baroda's headquarters in Mumbai, India, May 3, 2016. Photo Reuters/Danish Siddiqui.

The bank's Indian head office denies any wrongdoing in the affair. But interviews and documents obtained by reporters prove otherwise. The documents show that the bank's South African branch issued unapproved loan guarantees, quashed internal compliance efforts, and prevented regulators from learning about suspicious transactions in a way that benefited the Guptas' network.

This report reveals new details of a scandal that has rocked South Africa in recent months.

The Gupta brothers -- Atul, Ajay, and Rajesh, who immigrated to the country from India in the 1990s -- are accused of using their money and influence to pursue a project of "state capture," in collaboration with former President Jacob Zuma, to enrich themselves at the expense of taxpayers.

The scandal led to Zuma's resignation under pressure from his ruling party, the African National Congress (ANC), on February 14. Earlier on the same day, police raided the Guptas' Johannesburg mansion; an arrest warrant for Ajay has been issued. The three brothers, as well as the former president's son, Duduzane, are on the run and believed to be in Dubai.

Duduzane Zuma is accused of being a key player and beneficiary in the Guptas' financial dealings. His father appointed many of the key officials that made the family's schemes possible.

At the core of these was the South African branch of the Bank of Baroda. The documents obtained by reporters show the bank played host to hundreds of millions of dollars' worth of suspicious transactions.

One of the larger deals that appears in the transactions is the Guptas' irregular acquisition and allegedly illicit sale to themselves of a major South African coal mine.

The revelations in the documents follow the bank's announcement in mid-February that it was shuttering its South African operations.

Reporters have also learned that the head of Bank of Baroda's South African branch, Sanjiv Gupta, may face disciplinary action over the bank's business in the country. (He is not known to be related to the Gupta brothers.)

A senior Indian government official, who asked to remain anonymous because of the sensitivity of the matter, confirmed to reporters that the bank has asked the Central Vigilance Commission, the country's top anti-corruption body, to initiate penalty proceedings against Sanjiv Gupta, which could result in his dismissal.

Revolving Funds

PH-053

The three Gupta brothers have for years been major players in South African business. After immigrating from India, they ran a computer hardware company called Sahara Computers, named after their hometown of Saharanpur. But their business really started to grow after they developed a relationship with Jacob Zuma, who was then Deputy President, in 2003. Both parties benefitted from an arrangement in which the Guptas allegedly provided Zuma's family with financial support while he provided access to lucrative state tenders and appointed friendly officials. Since then, the Guptas have moved into the mining and media industries, eventually building an empire that made the family one of South Africa's richest.

Their rise has not been without controversy. Previous reporting by OCCRP has shown how the Gupta empire earned millions on the back of Transnet, the country's main transportation infrastructure firm. The Guptas' alleged large-scale raiding of South Africa's public purse has for years been a public preoccupation in the country, particularly after the details were made public in the 2016 release of a critical report, "State of Capture," by former public protector Thuli Madonsela.

Over the years, the Gupta family has run afoul of several South African banks, including Standard Bank, Nedbank, and ABSA, which all shut down their businesses' accounts, citing reputational risks. In recent years, the Bank of Baroda's South African branches, which the Guptas have used since 2005, took on a crucial role as the family's preferred financial institution.

Years of transaction records obtained by OCCRP and The Hindu, as well as internal documents and audits, shed new light on how exactly the Gupta family made use of the bank for nearly a decade.

Click here for selected graphs detailing transactions involving persons and companies relevant to this article.

The documents show a wealth of suspicious transactions among several of the Gupta's real firms, as well as a series of shell companies controlled by the family. A key Gupta associate who appears in many of the transactions is Salim Essa, a director and shareholder in some of the companies, who is seen as the financial architect of many of the deals. The transactions include a number of back-to-back loans and other transfers that have no apparent legal or business purpose but which appeared to be used to disguise the origin of the money. Especially large amounts moved in and out of Sahara, the firm at the apex of the Gupta empire.

Close to 4.5 billion rand (about US$ 532 million, based on an average exchange rate over 10 years) was transferred among just a handful of the companies between 2007 and 2017. As a whole, the amount of cash flowing through the Gupta accounts was so large that it dominated the transactions of the entire Bank of Baroda branch in Johannesburg.

In some cases, the significant benefit to the Guptas and their allies was clear. The Baroda account of Atul Gupta, for instance, shows that he received 57.3 million rand ($4.8 million) from Westdawn, one of the shell companies, in a single transaction on March 26, 2015 (while reporting taxable income of just 1 million rand ($80,000) two years prior). Some of the money enriched former President Zuma's son Duduzane, who held shares in a number of the companies that received large transfers. And the Gupta-controlled Westdawn provided Gloria Ngeme Zuma, one of the former president's wives, with a 160,000 rand ($12,300) monthly salary for a position she held at one of their firms.

But many of the transactions were more complicated. Their purpose may have been to disguise the origin of money as it entered the Gupta empire -- much of it obtained through friendly state companies and cozy contracts -- and to blend it together to the point that it could no longer be tracked. At least some of the funds that flowed through the bank ended up in accounts controlled by the Guptas as far away as the United Kingdom, Hong Kong, and even the United States.

Many of the transactions lacked adequate documentation about the purpose of the transfers, as is required in South African banking regulations. Other times, information was included, but didn't make sense. For example, on June 14, 2016, the Gupta-controlled Koorfontein Mine wired 100 million rand ($6.5 million) to a Gupta-controlled mining company called Tegeta for "[environmental] rehabilitation," meaning the repair of damage caused by mining activity. But Tegeta does not itself offer such services, which are typically handled by outside contractors, raising the question of the real purpose behind this transaction.

One particular technique shows up frequently in the transactions: Inter-company loans with no "apparent legal or commercial purpose." For instance, on Jan. 18, 2017, transactional paperwork shows that Trillian Management Consulting, at the time majority-owned by Gupta associate Salim Essa, loaned 160 million rand ($11.8 million) from its Baroda account to another Gupta company, Centaur Mining. The actual loaned funds passed through another similarly titled company, Trillian Financial Advisory. However, while the transactions

PH-054

describe a loan, no loan documentation could be found and there was no explanation for why the funds for the loan were provided by another company.

Internal documents also show that some of the funds originated with two state-owned companies: Eskom, an electricity utility, and Transnet, a railroad company. (The Guptas' dealings with Transnet were detailed in an earlier OCCRP report.)

By June 2017, Eskom alone paid 466 million rand ($36.3 million) to Trillian for "management and financial services" at a time that the company had few employees and could not have performed the work. Internal Baroda documents noted that bank employees filed alerts about several irregularities about the payments, including the fact that some were made on the same day as invoices were received (giving Eskom no time to assess the quality of the work) and the fact that, for some reason, some of the payments were made to accounts held by other companies.

Transfers stating "intercompany loan" as reason

No.	Entity transferring funds	No. of transfers	Total value of transfers (ZAR)	Entity receiving funds
1.	Koornfontein Mines	9	159,000,000.00	Tegeta Exploration and Resources
2.	Oakbay Investments	35	708,100,000.00	Tegeta Exploration and Resources
3.	Oakbay Investments	2	30,200,000.00	Idwala Coal
4.	Oakbay Investments	3	13,500,000.00	Infinity Media
5.	Oakbay Investments	25	576,321,190.41	Islandsite Investments 180
6.	Oakbay Investments	1	5,500,000.00	Shiva Uranium
7.	Oakbay Investments	2	14,200,000.00	TNA Media
8.	Oakbay Investments	26	380,200,000.00	Westdawn Investments
9.	Confident Concepts	5	174,400,000.00	Islandsite Investments 180
10.	Infinity Media	4	26,500,000.00	Oakbay Investments
11.	Islandsite Investments 180	30	655,788,000.00	Oakbay Investments
12.	Islandsite Investments 180	10	88,819,190.41	Confident Concepts
13.	Islandsite Investments 180	8	105,300,000.00	Sahara Computers
14.	Tegeta Exploration and Resources	26	303,900,000.00	Koornfontein Mines
15.	Tegeta Exploration and Resources	26	579,150,000.00	Oakbay Investments
16.	Tegeta Exploration and Resources	11	260,000,000.00	Optimum Coal Mine
17.	Tegeta Exploration and Resources	1	24,000,000.00	Westdawn Investments
18.	Trillian Management Consulting	1	160,246,000.00	Centaur Mining
19.	Westdawn Investments	4	142,000,000.00	Oakbay Investments
20.	Optimum Coal Mine	1	13,500,000.00	Koornfontein Mines
21.	Optimum Coal Mine	1	25,000,000.00	Tegeta Resources

Transactions flagged as "intercompany loans" involving companies owned or controlled by the Guptas. Infographic: OCCRP.

Despite all of the suspicious transactions, Baroda kept doing business with the two dozen shell companies controlled by the Gupta inner circle. The bank's employees dutifully filed suspicious activity reports (SARs), which banks are legally required to file with regulators whenever they see suspicious or potentially suspicious activity. On some days, they filed as many as half a dozen SARs related to the Guptas' transactions. However, Bank of Baroda managers often stepped in and voided the reports, marking the transactions as "genuine." As a result, most of the SARs never reached the South African Financial Intelligence Centre, the state body in charge of reviewing and acting on them.

Abdication of Responsibility

In 2016, the Baroda transactions spiked dramatically even as other South African and foreign banks closed out their own Gupta accounts amid negative headlines about the family. Tens of millions of dollars moved through the Guptas' Baroda accounts during that year.

Because the Bank of Baroda is a foreign bank, it needs a local sponsor bank to work in South Africa. That bank was NedBank. All transactions the Indian bank made used Nedbank's infrastructure. But this relationship made it possible for the two banks to shift responsibility for the Guptas' transactions to each other.

For example, Nedbank could perform due diligence on the foreign bank branch itself -- but did not have access to money moved between Baroda accounts. It was up to Baroda to check these clients and oversee those transactions. On the other hand, there was other information Baroda could not see, such as the origin of transactions made to Baroda accounts from external banks. Partly as a result, neither bank took responsibility for ensuring that the transactions were legitimate.

It remains unclear whether the Bank of Baroda ever reported any suspicious activities to South Africa's Finance Intelligence Centre. But one thing is apparent: Nedbank kept Baroda on as a client despite evidence that suspicious activities were taking place. Like other South African banks, Nedbank closed down their own Gupta family-related accounts, but shutting down Baroda, a bank the Indian government owns, would have been politically costly, an insider close to Nedbank told OCCRP and The Hindu.

This helped keep the Guptas in the money-moving business even as authorities circled in.

The Bank of Baroda continued to allow the Guptas' activities until January this year, when a South African court ordered it to share information about the accounts of more than 20 Gupta-linked companies. This was prompted by a Public Access to Information Request filed by the Helen Suzman Foundation, a local NGO. The bank has said it will release the records in a few weeks.

PH-055

Prepaying Corruption

The Bank of Baroda transactions related to Tegeta, the mining company, offers an instructive example of the questionable origin of some of the money that circulated within the Gupta accounts.

On April 13, 2016, Tegeta, a joint venture of the Guptas and Mabengela, a company owned by the former president's son Duduzane, received three deposits totalling 823 million rand ($65 million). The money arrived in Tegeta's account via several different Gupta-controlled accounts at the Bank of Baroda.

On the same day, Baroda bank employees filed four SARs against the Gupta's Sahara account. Four more alerts were filed the next day when new transactions came in. But sometime between April 13 and May 2016, Baroda officials nullified the alerts, pronouncing the transfers acceptable, which ensured that the Financial Intelligence Center did not discover them.

Much of the money flowing into Tegeta's Baroda account was South African taxpayer money that came from state-owned entities. From January 2016 through February 2017, Eskom, the state electricity provider, deposited over 1.8 billion rand ($143 million) into various Gupta accounts at Baroda.

Eskom was like a bankomat machine for the Guptas -- and there is evidence of high-level political involvement. Eskom executives like Anoj Singh and Brian Molefe had been handpicked by senior Gupta allies, like Public Enterprises Minister Lynn Brown, who themselves had been appointed by the president.

Two South African men read a newspaper detailing a financial scandal involving the Gupta family, October 2016. Photo: CC BY-NC-ND 2.0: Skatkat / Flickr.

Tegeta was a major Eskom subcontractor. In one 2016 deal, it was given a massive 564 million rand ($48 million) contract to supply Arnot, a large power plant, with six months of coal. Eskom had been purchasing coal for an average price of $19.40 per ton, but Tegeta received more than double that amount. It was the most expensive supply contract on Eskom's books. Money from this contract was among the millions that flowed into the Gupta's Baroda accounts.

Another deal involving Tegeta stands out: the company's purchase of the Optimum Coal Mine in April 2016.

Previously owned by Glencore, a multinational commodity trading and mining company, Optimum Coal was a major supplier of coal to Eskom, the country's electric utility. But there was a hitch: Eskom claimed that the Glencore coal was of a low quality and demanded 2 billion rand ($170 million) in penalties.

PH-056

Glencore said that, due to the fine, it was no longer profitable to supply Eskom and decided to sell the Optimum Coal company. With a huge penalty on its books that Eskom refused to waive, interested buyers were few.

Then, in December 2015, Tegeta announced that it would buy Optimum Coal for 2.1 billion rand ($160 million). South Africa's Mines Minister -- a known Gupta ally named Mosebenzi Zwane (who had been appointed by President Zuma) -- travelled to Switzerland to meet with Glencore and the Guptas. Shortly afterwards, the penalty was waived.

On December 18, 2015, Sanjiv Gupta, the Bank of Baroda's South African head, issued a letter of assurance from the bank on behalf of the Guptas for the full payment. India's Central Vigilance Commission is now examining whether it was in his powers to do so, according to a source.

But there was one more snag. On April 11, 2016, the Guptas informed Glencore that they were 600 million rand ($48 million) short of the sale price. South African banks had declined to lend to Tegeta, by then already perceived as a Gupta-Zuma scheme. Yet by 9 p.m. that night, in a wholly unusual move, Eskom agreed to "prepay" the Gupta companies 659 million rand ($52 million) for future work so that the purchase could be completed. The deal was, at best, an interest-free loan for the Guptas and Zuma. At worst, it was another plundering of public assets.

South Africa's President Jacob Zuma announces his resignation at the Union Buildings in Pretoria, South Africa, February 14, 2018. Photo: Reuters/Siphiwe Sibeko.

Bank of Baroda records show the Guptas using a series of transactions to pay a total of 1.8 billion rand ($144 million) for the mine. There is no record of what happened to the remaining amount.

Essentially, Tegeta had paid for much of Optimum Coal using taxpayer money from Eskom -- which had waived a fee that, according to the mine's previous owner, had rendered the venture unprofitable.

By 2017, the Gupta's deals had come under scrutiny, particularly the allegedly illegal payments made by state-owned entities like Eskom.

In August 2017, the Guptas announced that Tegeta had been sold for 2.97 billion rand ($225 million) to a Swiss company called Charles King SA. This was an unusual buyer for a mining company, having been formed in February 2011 as a clothing distributor with 50,000 Swiss francs ($53,500) in capital and managed by a financial services firm with a nominee director. An Emirati named Amir Zarooni, an alleged Gupta proxy, became the company's sole administrator in August 2017, at which time the company's registered activity changed simply to "trading."

If the deal in fact went ahead as described, the Guptas would have effectively paid the $225 million for Tegeta to a foreign proxy -- placing the money in Switzerland, a foreign tax haven, where it is beyond the reach of South African law enforcement.

PH-057

There was another financial windfall. When they purchased the Optimum Coal company from Glencore, the Guptas received 1.7 billion rand ($136 million) in "rehabilitation funds," where are meant to be set aside to mitigate environmental damage and used after the mine had closed. But, in violation of South African law, the Guptas took out loans against this money, moving the funds to their accounts at the Bank of Baroda, which allowed them to borrow nearly the same amount against the fund in early 2016.

The loan was allegedly approved by Minister of Mines Mosebenzi Zwane, yet another Zuma appointee. It took until November 2016 for the Bank of Baroda to void the loan. It is not known what the Guptas used the money for.

Days after former President Zuma resigned, Optimum Coal filed for a business rescue - a term describing a financially distressed company that is seeking external support to survive. Seven other Gupta-related businesses did too.

South Africans Will Pay. Will Anyone Else?

The South African authorities say they are seeking to recover as much as 50 billion rand ($4.07 billion) lost through the Guptas' deals.

In the meantime, the country is struggling. The government has announced plans to slash the national budget by tens of billions of rand, as well as raising taxes, including the VAT and fuel levy. Meanwhile, Eskom is so financially strapped that it has sought steep increases in electricity tariffs for South African consumers.

The Guptas and Essa did not respond to questions sent by reporters. Bank of Baroda officials in South Africa also did not respond to questions.

In a statement, Baroda's Indian head office said: "The South African operation of the Bank has always been and continues to be conducted in accordance with the laws and regulations of the home and host country regulators."

"To date, neither the South African regulators nor the independent auditors it has appointed to review these accounts and transactions have found that the Bank's South African territory engaged in any intentional wrong doing [sic] whatsoever."

Nedbank also denied any wrongdoing, saying, "In respect of all of our clients, including Bank of Baroda's SA branch, Nedbank has a responsibility to apply anti-money laundering regulations, 'know-your-client' procedures and report all suspicious transactions to the Financial Intelligence Centre. Nedbank has a robust system to comply with its know-your-client and suspicious transaction reporting obligations, and applies these rigorously to all our clients."

Sylke Gruhnwald contributed to this report.

This story is part of the Global Anti-Corruption Consortium, a partnership between OCCRP and Transparency International. For more information, click here.

Additional support was provided by Trust Africa.

Tweet Share

south africa India GuptaLeaks Bank of Baroda

Most recent

PH-058

Prosecutors Drop Investigation Into Millions Missing From Montenegro Bank

Prosecutors Drop Investigation Into Millions Missing From Montenegro Bank

Before Campaigning for Trump, Manafort Plotted to Rig Ukraine Telecoms Deal, Leaked Emails Show

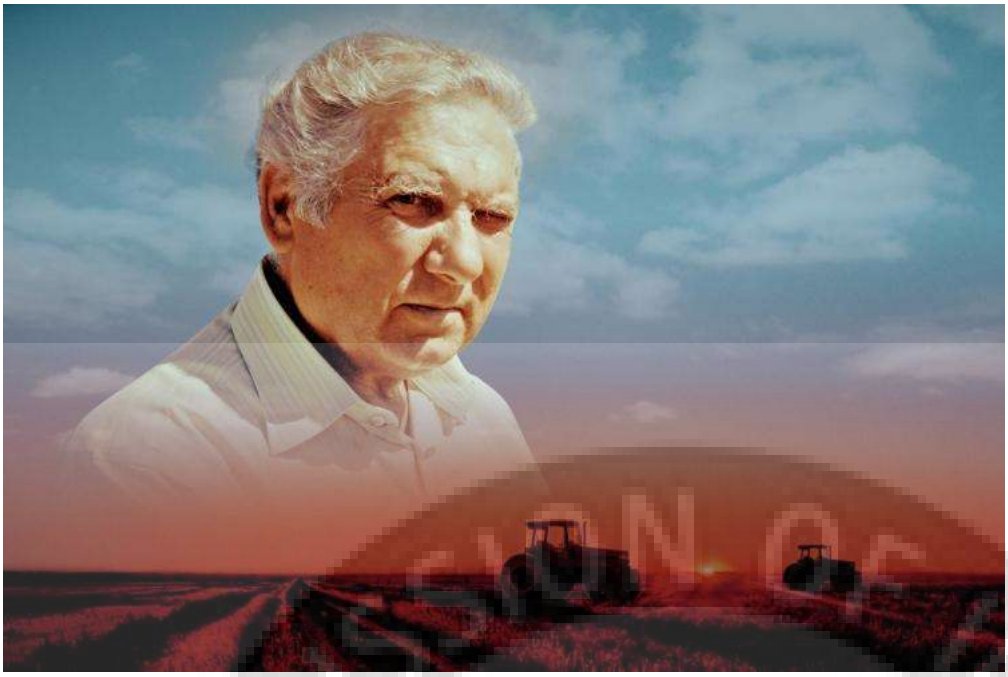
Before Campaigning for Trump, Manafort Plotted to Rig Ukraine Telecoms Deal, Leaked Emails Show

PH-059

Exposed: The Ukrainian Politician Who Funded Paul Manafort's Secret EU Lobbying Campaign

Exposed: The Ukrainian Politician Who Funded Paul Manafort's Secret EU Lobbying Campaign

PH-060



Two Tractors Outside Rivne, Ukraine

Two Tractors Outside Rivne, Ukraine

PH-061

Public Land, Private Hands

Public Land, Private Hands

Most read in this category

Subscribe to our weekly newsletter!

PH-062

DIY: The New Amphetamine Trade

DIY: The New Amphetamine Trade

Report: Russia Laundered Millions via Danske Bank Estonia

Report: Russia Laundered Millions via Danske Bank Estonia

PH-063

Operative for "Putin's Chef" Shares Secrets, Vanishes — Then Reappears and Retracts

Operative for "Putin's Chef" Shares Secrets, Vanishes — Then Reappears and Retracts

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-064

How a Meeting on a Yacht May Have Changed Kosovo's Political History

How a Meeting on a Yacht May Have Changed Kosovo's Political History

PH-065

Cyprus Records Shed Light on Libya's Hidden Millions

Cyprus Records Shed Light on Libya's Hidden Millions

© OCCRP Contact About Members History of OCCRP Staff
Board of Directors Awards Media Inquiries Our Supporters

Global Investigative Journalism Network

PH-066

A thematic review of trust and company service providers

May 2019

Executive summary

Background: trust and company services and money laundering risks

Money laundering is not a victimless crime. It is used to fund terrorists and facilitates drug dealers and people traffickers, as well as a range of other criminal activity. The credibility of solicitors and the services they offer makes them an attractive target for criminals, who want to launder their gains. Solicitors have a vital role - and opportunity - to help tackle the problem.

The creation and administration of trusts and companies on behalf of clients has been highlighted by the government as one of the legal service areas at highest risk of exploitation by criminals[1]. We agree with this assessment and it is reflected in our sectoral risk assessment. We have produced this document to set out information on money laundering and terrorist financing risks (/sra/how-we-work/reports/aml-risk-assessment/) that we consider relevant to those we supervise.

Trusts and companies are attractive to money launderers because individuals can:

- obscure the beneficial ownership and control of assets and wealth
- create and control multiple legal entities at a relatively low cost
- create complex and opaque structures
- operate across multiple jurisdictions
- avoid tax or duties.

They are the vehicle of choice for the legitimate investment and business world, however criminals may use them to add a veneer of legitimacy to illegal transactions.

Cookies are small text files our website stores on your device to improve your experience. Please consent to our use of cookies.

OK, I UNDERSTAND

Tell me more about cookies (https://www.sra.org.uk/privacy)

PH-067

The government is committed to disrupting and stopping money launderers and continuing to develop anti-money laundering (AML) and counter terrorist financing (CTF) requirements to monitor, assess and mitigate the risks posed by these vehicles[2].

Our role

In July 2018, our Risk Outlook highlighted our growing concern about the risks and challenges posed to the profession by those looking to launder the proceeds of crime and finance terrorism. We explored this further in our Autumn update, where the concern was raised as a priority risk. Our interest in this area continues to intensify and is reflected in our significant, ongoing activities.

As a professional supervisory body, we have a statutory duty to make sure those we regulate assess risks and take proactive steps to mitigate and respond to money laundering issues. We must also take "effective, proportionate and dissuasive disciplinary measures[3]" where firms do not reach the required standard.

Our activities in this area are monitored by our supervisor, the Office for Professional Body Anti-Money Laundering Supervision (OPBAS).

What we did

In 2018 we reviewed 59 law firms in England and Wales that told us they carried out trust and company service provider (TCSP) work. We had initially planned to review 60, but upon visiting one firm we found they did not carry out this work. We met with firms, money laundering reporting officers (MLRO), money laundering compliance officers (MLCO) and fee earners.

At each firm, where possible, we reviewed two TCSP files. This report features findings from 115 file reviews.

We looked at each firm's compliance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017). The MLR 2017 place certain responsibilities on firms and individuals offering services most likely to be targeted by money launderers, including TCSPs. Around two thirds of the firms we regulate fall within scope of the MLR 2017.

This report summarises what we found. It builds on our two previous money laundering reviews in 2016 and 2017. These looked more generally at how law firms were tackling money laundering. The 2017 review also considered how they were responding to the government's money laundering regulations.

Cookies are small text files our website stores on your device to improve your experience. Please consent to our use of cookies.

OK, I UNDERSTAND Tell me more about cookies (https://www.sra.org.uk/privacy)

PH-068

Headline summary

- In this review we found most law firms who carry out TCSP work are adequately meeting their obligations to tackle money laundering. Yet a significant minority are not doing enough, with some falling seriously short.
- We found no evidence of actual money laundering or that firms had any intention of becoming involved in criminal activities. Breaches of the MLR 2017 and poor training or processes could, however, mean firms are unwittingly assisting money launderers.
- Any AML system is an interdependent collection of policies and processes. Where one of these areas fails, it weakens the strength of the entire system. Areas where we had particular concerns included firm risk assessments, file risk assessments and the overall adequacy and availability of policies, controls and procedures.
- A firm risk assessment is required in legislation and should be the backbone of a firm's AML approach. We found that too many firms' approach was inadequate. More than a third of firms' (24) assessments did not cover areas required in legislation, this included a small number (four out of the 59 firms we visited) that had no risk assessment at all.
- Firms need to understand who their client is and what money laundering risks they pose. Our concerns in this area included inadequate processes to manage risks around politically exposed persons (PEPs) - an issue in around a quarter of firms. Some firms are also not doing ongoing customer due diligence (CDD), which is particularly important for TCSP work where the client can change. We did, however, find that 15 firms had turned down client instructions, with clients being evasive one of the main reasons.
- Most firms provided specific training about trust and company work and beneficial ownership. Poor training leads to poor compliance. Seven firms did not provide training on these topics and we have referred five of these into our disciplinary processes for breaches of the MLR 2017.
- Only ten firms - a sixth of our sample - had submitted suspicious activity reports (SARs) in the last two years. This tallies with concerns raised by the National Crime Agency (NCA) that generally law firms are not being proactive enough in looking to identify and then report suspicious activity.
- As a result of this review, we have referred 26 firms into our disciplinary processes. We will judge each case on its facts and will be keen to see evidence that firms are moving swiftly to comply with their obligations. We will take strong action against firms where we have serious concerns that they could be enabling money laundering, and/or those who fail to address our concerns promptly.
- Other action we are taking includes:

Cookies are small text files our website stores on your device to improve your experience. Please consent to our use of cookies.

OK, I UNDERSTAND | Tell me more about cookies (https://www.sra.org.uk/privacy)

PH-069

- publishing a warning notice highlighting our concerns, particularly in relation to firms' risk assessments
- writing to 400 firms asking them to demonstrate compliance with the MLR 2017, focused on the approach to risk assessments
- setting up a new dedicated AML team in the SRA, with increased resource to monitor and ensure compliance in this area.

Summary of findings by area

Most firms had appropriately assessed, monitored and mitigated the risks inherent within TCSP work. However, a significant minority of firms must improve across various areas.

Identifying and assessing risk

- Four firms failed to produce written firm risk assessments. This is a mandatory document and informs each organisation's controls and mitigations.
- Twenty-four firms had an inadequate file risk assessment that failed to cover various areas required by statute.
- Twenty firms were not able to show that they had specifically addressed TCSP work in their firm risk assessment
- Thirty-nine firms specifically covered TCSP work in their firm risk assessment.

Policies, controls and mitigation

- File reviews revealed 21 occasions where firms were unable to show they had continued to review CDD and keep it up-to-date.
- PEPs featured on six files we reviewed.
- We were only satisfied with 45 of the PEP processes we reviewed.
- We found no specific issues about the application of enhanced due diligence (EDD).
- AML training was provided at most firms but 17 firms failed to provide training about TCSP work. Of that 17, seven firms also failed to provide training about beneficial ownership.
- Firms had very low numbers of internal suspicious activity reports (ISARs). These are reports about potential money laundering concerns raised by employees with the MLRO or

Cookies are small text files our website stores on your device to improve your experience. Please consent to our use of cookies.
OK, I UNDERSTAND
Tell me more about cookies (https://www.sra.org.uk/privacy)

PH-070

deputy.

- Only 10 firms had submitted SARs in the last 24 months.
- Fifteen firms had turned down TCSP instructions for various reasons.

Open all

Next steps

Introduction

Identifying and assessing risks

Policies, controls and mitigation

Conclusion

NOTES

Print this page

Save as PDF (/pdfcentre/?id=1616884285)

Regulated population statistics (/sra/how-we-work/reports/statistics/regulated-community-statistics/)

Consumer research (/sra/how-we-work/consumer-research/consumer-research/)

Assigned risks pool (/sra/how-we-work/reports/assigned-risk-pool/arp-enforcement-review/)

Cookies are small text files our website stores on your device to improve your experience. Please consent to our use of cookies.

OK, I UNDERSTAND

Tell me more about cookies (https://www.sra.org.uk/privacy)

PH-071

For law professionals

SRA Handbook (/solicitors/handbook/welcome/)

Guidance (/solicitors/guidance/)

Investigation and enforcement (/solicitors/enforcement/)

Firm-based authorisation (/solicitors/firm-based-authorisation/)

Supervision (/solicitors/supervision/)

Resources (/solicitors/resources/)

Qualified Lawyers Transfer (/solicitors/qlts/)

Good standing and certificates (/solicitors/certificates/)

For the public

Who we are (/consumers/who-we-are/)

Finding and using a solicitor (/consumers/find-use-instruct-solicitor/)

Check a solicitor's record (/consumers/solicitor-check/)

Problems with a solicitor (/consumers/problems/)

Frequently asked questions (/consumers/faqs/faqs-for-consumers/)

Scam alerts (/consumers/scam-alerts/)

Students

Academic stage (/students/academic-stage/)

Legal Practice Course (/students/lpc/)

Resources (/students/resources/)

Trainees

Training Contract (/trainees/training-contract/)

Period of recognised training (/trainees/period-recognised-training/)

Professional Skills Course providers (/trainees/professional-skills-course-providers/professional-skills-course-providers/)

Admission (/trainees/admission/)

Resources (/trainees/resources/)

About us

Equality and Diversity (/sra/equality-diversity/)

How we work (/sra/how-we-work/)

Decision making (/sra/decision-making/)

Consultation and discussion (/sra/consultations/)

Cookies are small text files our website stores on your device to improve your experience. Please consent to our use of cookies.

OK, I UNDERSTAND Tell me more about cookies (https://www.sra.org.uk/privacy)

PH-072

Cookies are small text files our website stores on your device to improve your experience. Please consent to our use of cookies.

OK, I UNDERSTAND Tell me more about cookies (https://www.sra.org.uk/privacy)

Transparency International - Unit

transparency.org/country/GBR

OUR GLOBAL MOVEMENT POPULAR CONTENT

TRANSPARENCY INTERNATIONAL

HOME WHO WE ARE WHAT WE DO GET INVOLVED NEWS DONATE Search

Corruption Perceptions Index 2018

Rank 11 / 180

Score 80 / 100

Contact our chapter

Building on the EU directive for whistleblower protection

HELPDESK ANSWER

Interagency coordination mechanisms: improving the effectiveness of national anti-corruption efforts

EU countries' chance to lead on whistleblower protection

HELPDESK ANSWER

Regulating Private Sector Corruption

Three ways to stop money laundering through real estate

Around the world, buying property is a favourite method for the corrupt to launder their ill-gotten gains. However, there are concrete measures that make it significantly more difficult for the corrupt to stash their dirty money in real estate.

Trade unions and civil society call on G20 to protect whistleblowers

HELPDESK ANSWER

Models of donor coordination for managing multi-donor inputs

Why corruption matters in

PH-074

KPMG LLP

KPMG South Africa executives dismissed over Gupta scandal

Internal investigation finds auditing firm missed red flags

Joseph Cotterill in Johannesburg and Madison Marriage in London SEPTEMBER 15 2017

The South African scandal engulfing President Jacob Zuma and the billionaire Gupta family spread deeper into the global professional services sector on Friday when eight senior executives were dismissed from KPMG's division in the country.

The biggest political scandal to face South Africa since the apartheid era has already triggered the collapse of British PR firm Bell Pottinger and forced McKinsey, the consultancy firm, to launch an investigation into its work in the country.

Public outrage about the Guptas' role in South African politics intensified in June when leaked emails fuelled fears the family was exploiting its friendship with Mr Zuma to win state contracts and manipulate political appointments. The family and Mr Zuma deny the allegations.

The departures at KPMG came after an internal investigation found the accounting firm had missed red flags in its auditing of companies owned by the Gupta family. The auditor said on Friday that KPMG's South Africa division — the firm's largest business in Africa — had received warnings "regarding the integrity and ethics of the Guptas" that were not acted upon, and which should have led to it cutting ties with the family sooner. South Africa is arguably KPMG's most important market in Africa, as it boasts the continent's most industrialised economy, its biggest companies and its largest stock market.

KPMG audited companies linked to the Guptas for 15 years but ended its relationship with them in March 2016 as the political scandal over the family's links to Mr Zuma deepened.

PH-075

Trevor Hoole, the KPMG South Africa chief executive who resigned on Friday, admitted last month that the group "should have stopped working for the Gupta companies sooner than we did".

KPMG may find that it has gotten caught with its hand in the cookie jar just as the lights have been turned on

Opposition parties and civil society groups, who have repeatedly accused Mr Zuma of running a state system riddled with corruption and cronyism, have turned their focus on global companies tainted by the controversy.

Save South Africa, a civil society group, has accused KPMG and Bell Pottinger of playing a "central role in facilitating state capture". The campaign group has urged KPMG and McKinsey clients to drop the firms over the issue.

Sygnia, the South Africa-listed asset manager, dropped KPMG as its auditor in July because of its work with the Guptas while Barclays Africa Group is reviewing its relationship with the auditor.

Growthpoint Properties, one of South Africa's largest real estate companies, said it was monitoring the outcome of the local regulator's investigation of KPMG's work in the country before deciding whether to stay with the firm.

The UK PR industry body's decision to expel Bell Pottinger after its role was exposed following a complaint by the Democratic Alliance, the main opposition, was hailed as a huge victory for South Africans angered by the lack of action taken in their own country against those implicated.

Many South Africans have little faith in the independence of state security agencies and the national prosecution authority. Mr Zuma, who has 783 counts of graft, fraud and money laundering hanging over him, is a ruthless political survivor who has shrugged off a string of scandals since taking office in 2009.

KPMG has become central to the scandal over the Gupta family since the leaked emails showed its South African office allowed a Gupta-owned company, Linkway Trading, to treat spending on a 2013 Gupta family wedding as a business expense.

Moses Kgosana, a KPMG executive, referred to the wedding in the emails as the "event of the millennium" and four KPMG partners attended.

KPMG on Friday also disavowed its work on a 2015 report used by state investigators to try to discredit Pravin Gordhan, a former finance minister among the strongest critics of the Guptas. Mr Gordhan, who alleged corruption at state-owned companies, was fired by Mr Zuma this year.

PH-076

KPMG said it would pay the R40m ($3m) it had earned from auditing Gupta-owned companies since 2002 to anti-corruption charities. It will also pay back R23m earned from writing the 2015 report used to support claims that Mr Gordhan set up a rogue tax spying unit, when he headed the revenue service. KPMG said the report should "no longer be relied upon".

The internal investigation was conducted by KPMG International — the big four accounting firm's global arm — with the assistance of a South African expert on tax laws.

"Despite the deficiencies in the audit work, KPMG International found no evidence of dishonesty or unethical behaviour" by partners working on Gupta company audits, KPMG South Africa said.

The auditing firm added that managers of the Gupta-linked companies had responded "misleadingly and inadequately" to KPMG's inquiries "about the nature of related-party relationships and the commercial substance of significant unusual transactions".

KPMG has denied that it "was involved in, or condoned, any alleged money laundering activities" connected to Gupta-owned companies or facilitating offshore tax evasion.

Karthik Ramanna, professor of business and public policy at the University of Oxford's Blavatnik School of Government, pointed out that KPMG had ethics issues before, including a 2005 settlement with the US government over fraudulent tax shelters.

"But times are different today. There's a deep level of populist disenchantment with business and government leaders across the world," he warned. "KPMG may find that it has gotten caught with its hand in the cookie jar just as the lights have been turned on."

Additional reporting by Andrew England

Copyright The Financial Times Limited 2019. All rights reserved.

PH-077

OPINION

ISMAIL MOMONIAT: When will Bain tell the whole truth about its role a

Public relations gloss cannot hide the fact that it plotted to undo the hard work put into building a world-r

01 JULY 2019 - 05:06 *by* ISMAIL MOMONIAT

Picture: SUPPLIED

Bain & Company partner Athol Williams's article "Jump into the fire to quell corporate pyre", publis company when "many are running from Bain", but fails to answer the real question facing him and t tell the whole truth about its role in attempting to capture and destroy the capacity of the SA Reve

Bain's contribution in facilitating state capture in SA is unforgivable. We must not be blinded by Ba in "restructuring" Sars in 2014 not only nearly destroyed Sars but also destroyed the livelihood of m

The damage to Sars's capacity to collect revenue not only significantly damaged our fiscal framewo devastating inequality that defines our nascent democracy. Bain deliberately plotted to reverse the morality and Sars into a world-renowned revenue collection agency.

So serious were its actions that the Nugent commission recommends criminal prosecutions agains "premeditated offensive against Sars, strategised by the local office of Bain & Company Inc, locatec Moyane to seize Sars ... Mr Moyane's interest was to take control of Sars. Bain's interest was to mak

In plotting to do this, Bain's head in SA, Vittorio Massone, had at least seven meetings with Moyan president Jacob Zuma from August 11 2012, some at Nkandla. Is this the way Bain wins contracts in developing countries only?

" If Bain wants truly to make reparation, then it should give to South Africans what they want and r

- Judge Bob Nugent

PH-078

The "remedial plan" announced last week by Bain, including a new chair for its Africa oversight bo
insult to all South Africans. It confirms the company's unrepentant stance in obfuscating its liability
returning "all fees plus interest" and making "leadership and governance enhancements" are enoug

This is in line with its evasive attitude to the Nugent commission, which concluded that "Bain has r
"an extraordinary approach to be adopted by a major international consultancy that claims its com

Judge Bob Nugent was clear: "If Bain wants truly to make reparation, then it should give to South A
they should have, which it has steadfastly refrained from doing. Payment of money without prior d
marketing instead."

Williams's article confounds expectation by not addressing the Nugent commission's findings abou
Bain has withheld, and continues to withhold, information from the commission than the prelimina
apparent that even he has yet to be told where the truth lies". Can Williams tell us when Bain will p

The Zondo and Nugent commissions have shown how too many multinational consultancies voraci
for their own ends. Williams, a business ethics expert, will agree that multinational companies can
between their parent countries and their foreign operations.

Its blatantly predatory behaviour in SA calls for all Bain's public sector contracts to be scrutinised f
including for possibly transgressing US foreign corrupt practices laws. Massone (and those respon
face any possible charges.

Williams has not so much "run towards the fire when all logic dictates that I should be going in the
into fire. Perhaps the image of a funeral pyre Williams invokes is apt: something remains buried, wa
changed its spots, and he ain't no firefighter!

• *Momoniat is deputy director-general at the Treasury.*

SPONSORED

Want to make profit online?

VICI MARKETING | MARKETINGVICI.COM »

ARTICLE NOT AVAILABLE FOR PRINTING

NOT SUBSCRIBED TO "FINANCIAL TIMES"

(www.ft.com)

Acacia Mining falls 4% on report of SFO probe, Financial Time, 17 December 2018,

https://www.ft.com/content/7d585320-01f2-11e9-9d01-cd4d49afbbe3

COMMISSION OF INQUIRY INTO STATE CAPTURE

FOOT NOTE EXPLANING "JAVELIN-THROWING"

In South Africa a variant of this private-state collaboration in corruption is referred to as 'javelin-throwing', where corrupt officials sign off on a lucrative tender, knowing that they will be leaving the employ of government in the near future and that they will become part of the benefitting company either as a director or as a senior employee.

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-081

The US and South Africa are stronger together

I will especially strive to help more women to achieve their professional goals, writes new US ambassador to SA **Lana Marks**.

EXCLUSIVE: Gupta-linked train company in R5bn rip-off

2018-03-23 10:16

Pieter-Louis Myburgh

news24

The Chinese rail giant that allegedly paid bribes of over R5bn to the Guptas has told the state it will no longer invest R5bn in the local train industry.

In a rip-off deal reminiscent of the disastrous "offsets" that were used to justify the arms deal, China South Rail (CSR) recently applied to the government for an exemption from its local content obligations worth R5bn in its ongoing supply of new locomotives to Transnet.

In a surprising coincidence, this is almost exactly the same amount as the questionable "fees" that CSR allegedly agreed to pay Gupta-linked shell companies after it clinched contracts from Transnet worth R25bn.

Former Transnet CEO Brian Molefe at the signing of a new deal to build locomotives for Transnet Freight Rail on March 17, 2014 in Johannesburg. (Photo by Gallo Images)

Multimedia · User Galleries · News in Pictures
Send us your pictures · Send us your stories

The department of trade and industry (DTI), which is tasked with ensuring that the policy objectives included in large government tenders are achieved, rejected the exemption request.

But the DTI has apparently lost all hope that CSR can still achieve a local content score of 60%, as is required by the Transnet contract.

"The challenge with the CRRC (CSR) project is that [it] has progressed to the extent that any development work or investment to be done with or by the local manufacturers might not be financially feasible," the DTI told News24.

This sentiment is shared by many business people from the local rail industry.

Transnet's massive tender for 1 064 new locomotives, which was concluded in 2014, came with strict local content and supplier development obligations. These requirements are supposed to help create jobs and grow the local economy.

The first 166 of 359 locomotives thus far delivered by CSR to Transnet as part of the 1 064 project has a local content score of only 33%, according to figures supplied by the company itself. Some industry insiders are skeptical, saying even 33% local content seems unlikely.

News24 can today reveal that CSR earlier this year submitted a request to the department of trade and industry (DTI) with a detailed list of 53 components. CSR claimed that it was either unable to find local suppliers for these components or that the "technology licensing" for these products was not available in South Africa.

READ: #GuptaLeaks: The great train robbery Part 2 – The choo-choo switcheroo

The DTI later confirmed that these components were valued at R5bn.

MOST READ | NEWS IN YOUR AREA | TOP LIFESTYLE

Ex-Ireland lock: Springbok World Cup win tainted by drug abuse
Guscott suggests law change to nullify Bok 'bomb squad'
Eddie Jones on where he erred in World Cup final
9 Springboks in Barbarians squad
FACT: Rassie now 'loses control' of most top Boks

More..

PH-082

Thandi Phele, the DTI's chief director for metal fabrication, capital and rail transport equipment. (Pieter-Louis Myburgh,News24)

Asked whether CSR was trying to backtrack on its local content obligations because of the "fees" it allegedly had to channel to the Guptas, the company said it couldn't comment on "untested allegations".

"What we can assure you is that CRRC (CSR's parent company), as one of the major state-owned companies in China, is committed to operate in compliance to the laws, rules and regulations of the republic of South Africa," it added.

"CRRC, the Chinese government and other law enforcement agencies are also investigating the allegations which were contained in the leaked emails and we will cooperate with investigations in South Africa and China," said CRRC.

CSR merged with fellow Chinese state-owned Original Equipment Manufacturer (OEM) China North Rail (CNR) to form CRRC after the two landed the lions' share of Transnet's R50bn tender.

For practical purposes, however, CSR and CNR are delivering their trains to Transnet as separate entities.

CSR's slice of the 1 064 tender is a R18.1bn contract for 359 class 22E electric locomotives. It also clinched two earlier deals for 95 and 100 electric locomotives, valued at R2.7bn and R4.4bn respectively. In all, CSR is supplying Transnet with 554 trains at a cost of more than R25bn.

#Guptaleaks 'kickbacks'

One of the biggest scandals that emerged from last year's #GuptaLeaks reports was amaBhungane's revelation that CSR had apparently entered into alleged kickback agreements in relation to the Transnet tenders.

Documents sourced from the leaked emails showed that Gupta-linked companies in the United Arab Emirates (UAE) were set to receive a staggering R5.3bn in "fees" emanating from CSR's Transnet contracts.

CSR's recent request to be exempted from sourcing local components worth R5bn set off alarm bells in the local rail industry.

"It is like CSR now wants a discount on its local content obligations because it had to pay the Guptas so much money to open up these contracts with Transnet," said one of several industry insiders News24 spoke to.

Two weeks ago, a collection of representatives from the local rail industry met with CRRC, CSR's new parent company, at the Birchwood hotel in Boksburg. Officials from Transnet and the DTI were also in attendance.

/News

WATCH | Shot security guard airlifted to hospital after Hurlingham house robbery

TRAFFIC ALERTS

Western Cape

TRAFFIC

Cape Town 12:12 PM
Road name: N1 Inbound
Inbound

Kuils River 12:12 PM
Road name: R300 Northbound
Northbound

More traffic reports traffic24

Daily Lotto: One winner on Tuesday
2019-11-12 21:18

Click here for the full list of lottery results

JOBS IN CAPE TOWN [change area]

Jobs in Western Cape region

C# Developer
Cape Town
Mass Staffing Projects
R35 000.00 - R75 000.00 Per Month

PH-083

Representatives from CRRC, Transnet's Chinese trains supplier, and other delegates at a recent engagement with local industry. (Pieter-Louis Myburgh, News24)

ALSO READ: EXCLUSIVE: Transnet's new Chinese locomotives 'fail first test'

What started as a cordial session ended with some audience members – mostly owners or representatives of local companies with a footprint in the rail sector – openly showing their disgruntlement with CSR's handling of the local content issue.

One audience member shouted that "corruption" had ruined the local industry's chances of participating in the contract in a meaningful manner.

The DTI says it rejected CRRC's request because the OEM needed to make a greater effort to find local suppliers.

"The above exemption is the only request received to-date from CRRC (CSR), which has been rejected with the recommendation that the OEM intensifies its effort to find suitable local suppliers to locally manufacture and supply the required components in the bid to reduce the import content," said the DTI.

"Following the engagements with potential local suppliers and the session held on 12 March, CRRC has subsequently withdrawn the [request for] exemption," added the DTI.

CSR remains committed

CSR claims that its problems with reaching the required local content threshold is partly the result of shortcomings in the local industry.

"At the beginning of the project, we had more components that we found out after thorough supplier evaluation that the local suppliers will have problems in supplying us with because of not meeting our requirements (quality, speed of delivery and cost)," stated CSR.

However, the company says it remains committed to achieving its local content targets by the time it delivers its last locomotive to Transnet.

"After continuous engagement with local suppliers, the list [of possible exempted parts] was reduced to about 50 components. But since we have started implementing our localisation strategy in partnership with Transnet and under the auspices of DTI, we have stop pursuing the requests for exemptions," said the company.

"We are committed and confident that we will meet our contractual localisation targets through our latest strategy."

CSR says it has qualified 52 local suppliers that will supply an estimated 5 602 materials and components at a combined contractual value of just under R11bn for the duration of the Transnet class 22E project.

READ MORE: #GuptaLeaks: The great train robbery - Part 1: the Zurich tryst

Asked who these qualified local suppliers were, CSR responded as follow: "We can gladly share the information with you, but we will have to get permission from all affected local suppliers first."

Transnet says it is the responsibility of the South African Bureau of Standards (SABS), which was appointed by the DTI as the project's official local content verification agency, to ensure that the OEMs honour their local content commitments.

Hire Resolve
R420 000.00 - R780 000.00 Per Year

PA to Regional Manager Sales
Cape Town
MPC Recruitment (PE/EL)

BROWSE MORE CAPE TOWN JOBS...

East London Jobs | Call Centre Jobs
KwaZulu Natal Jobs | Sales Jobs
Limpopo Jobs | Human Resources Jobs

Register your CV...
Get Job alerts in your e-mail...
RECRUITERS – Advertise your jobs here

PROPERTY [change area]

News24.com
6,921,083 likes

Like Page Learn More

Be the first of your friends to like this

PH-084

which it has been engaging with the OEMs and their suppliers to monitor the local content reported," says Transnet.

The DTI admits that the verification process has been hampered by problems.

"In the 1 064 rolling stock procurement programme, the verification process is still ongoing in the midst of funding challenges and government budgetary constraints," said the DTI.

Do you have information for our investigative journalists? Send an email to tips@24.com

Read more on: transnet | china | gupta family | guptas

Paid Content

The Wireless Earphones Everyone in South Africa is Talking About

techgadgetdiscounts.com

Play this for 1 minute and see why everyone is addicted

Throne

[Photos] Meet The Spouses Of The World's Richest Billionaires

JOL

Joburg Wife Turns From Rags To Riches

SM-Invest

U.S. Goverment Announces Opening of the Registration for the Green Card Lottery!

U.S Green Card - Free Check

How to Open a Tin Without an Opener | Cleanipedia

Cleanipedia South Africa

More from

Mom of teen shares hospital image of her daughter on life support after her lungs…

'I want to sing for my mother'

WATCH: Faf 'Speedo crew' steals the show during the…

'Rogue' UKZN lecturer fired

Trial of student who received R14m of NSFAS…

Paid content

PH-085

[Photos] Woman Kept Hearing Strange Noises From Behind The Wall, Look What…
The Primary Market

[Photos] Two Brothers Discover 220-Year-Old Oak Island Treasure
JOL

More from

PICS | Durban highway closed as flooding, heavy rains wreak havoc

Angus Buchan apologises for saying only 'Jewish and Afrikaans people' have…

More from News24

Recommended by

Gospel picnic to pray for a safe festive season

Promising soccer player, 13, hit with brick on Guy Fawkes off life support

Mangaung Metro ba

'Overworked' Zuma out of hospital, thanks supporters for well wishes

Facebook apologises after black workers complain of bias

Zambia's president denies stifling opposition

COMMISSION OF INQUIRY INTO STATE CAPTURE

Other Stories in South Africa...

SAA: Unions have issued strike notice

PH-086

Richard Branson apologises for all-white photo in South Africa
After a blunder in South Africa, the billionaire moved on to even more controversy in Australia.

Relative identified as person of interest in murder of Jesse Hess and her grandfather
A relative has been identified as a person of interest in the murder of Capetonian Jesse Hess and her grandfather Chris, the former University of the Western Cape student's family has confirmed.

INSIDE NEWS24

How to make BLT potato skins
Potato skins are given a fun twist with a savoury egg custard and salsa.

Fourways beauty therapist helps cyberbullied cashier
"A bit of kindness goes a long way."

5 health benefits of cayenne pepper
Sprinkles cayenne over entire life

Parents can opt out of the new sex ed lessons
Motshekga says parents can opt out of the LO curriculum.

SERVICES

Press Code
We subscribe to the Press Code.

E-mail Newsletters
You choose what you want

News24 on Android
Get the latest from News24 on your Android device.

Terms and Conditions
24.com Terms and Conditions - Updated April 2012

© 2019 24.com. All rights reserved.

iab. south africa

This document is not available for inclusion in this bundle as it was not made available to the State Capture Commission nor is it available from public sources.

N.Mokeshi (HOD FSHS) submission to Free State Provincial Legislature

4 August 2015

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-088

PIETER-LOUIS MYBURGH
author of the bestselling *The Republic of Gupta*

GANGSTER STATE

Unravelling Ace Magashule's Web of Capture

PART III

THE R1-BILLION HOUSING SPLURGE

PH-090

‘Bring your people’

When Ace Magashule became Free State premier in 2009, he almost immediately began meddling in the affairs of the provincial departments with the largest budgets. One of those was the Free State Department of Human Settlements (FSHS), which is primarily tasked with providing low-cost housing to the province’s poorest citizens.[1] The FSHS became the site of such rampant looting by the Magashule capture network that it deservedly takes up a comparatively large portion of this book.

Let’s start with the province’s R1-billion Reconstruction and Development Programme (RDP) scandal from around 2010. This sordid saga is underpinned by a toxic combination of mismanagement and corruption, and Magashule’s fingerprints are all over it.

Earlier media reports exposed the involvement of a few politically connected individuals. But Magashule’s cronies escaped scrutiny and his own role in engineering this financial disaster remained under wraps, thanks to the department’s well-orchestrated management of the scandal’s fallout, which included selective legal proceedings that deliberately shielded Magashule’s friends and associates from exposure and financial liability. Most alarmingly, it appears Magashule may have directly participated in a wide-ranging cover-up to suppress the true facts by roping in a private forensic firm owned by a former government spy boss to ‘investigate’ the saga. This firm allegedly took hold of key documents and evidence, and subsequently prevented the Special Investigating Unit (SIU), which had also been tasked with

probing the issue, from accessing these important materials. As a result, the public was kept in the dark about Magashule and his cronies' apparent involvement in one of the largest low-cost housing scandals this country has ever seen.

FH-091

For the first time, this book exposes how scores of politically connected people benefited from a R1-billion spending frenzy that left in its wake hundreds of unfinished or poorly constructed RDP houses. Some of Magashule's closest associates pocketed money without completing their projects. And that is just the tip of the iceberg.

While studying the 2010 contracts, I stumbled upon records that detail the full, shocking extent of the capture and rot at the provincial Department of Human Settlements during Magashule's reign as premier. In a period of nearly a decade, the FSHS channelled contracts for new houses worth more than R2 billion to a band of businesspeople linked to or associated with Magashule. There is also evidence to suggest that he punished former political allies who had abandoned his camp by stopping the flow of RDP contracts to companies owned by or linked to them. In effect, a picture emerges that Magashule determined the direction of the department's money flows by acting as its de facto boss.

From a taxpayer's perspective, the Free State's low-cost housing programmes under the Magashule administration should elicit great anger. Many of the preferred contractors failed to deliver houses. Others constructed houses replete with shoddy workmanship and substandard materials. In the worst instances, houses collapsed or were of such poor quality that they needed to be demolished and rebuilt by other contractors.

Among this coterie of cronies were politicians who once sided with

Magashule in the ANC's factional battles, former business partners, colleagues in the provincial government and local legislature, and friends from his hometown. Even his daughter later tapped into the scheme.

PH-092

This wholesale capture of the province's housing budget was achieved by staffing the FSHS with people who could be trusted to act on Magashule's orders. Current and former department insiders attested to a government environment in which the premier loomed in the background to ensure that his friends and associates got the most lucrative housing contracts. 'Ace has spoken,' one former department staffer was told by his superior when he queried a 2012 contract awarded to a known Magashule ally without a tender process.

The premier's meddling, detailed in subsequent chapters of this book, appears to have forced department officials to override or ignore the rules and laws that govern how the state should spend its money. This reckless disregard for prescribed procurement standards is reflected in reports by the auditor-general, which show that the department incurred irregular expenditure totalling a jaw-dropping R7 billion in the nine years that Magashule ruled over the Free State.[2]

To put this into context, in 2013/14 the Gauteng Department of Human Settlements spent R4.2 billion, of which R461 million, or roughly 10 per cent, was found to be irregular.[3] In the same year, the much smaller FSHS spent about R1.5 billion, but managed to rack up irregular expenditure of R857 million, or 57 per cent of total spend.[4]

And 2013/14 was a relatively good year. In some financial years, as much as 80 (2015/16) and even 90 per cent (2011/12) of the department's expenditure was classified as irregular by the auditor-general.[5] The main culprits appeared to be contracts for housing

projects that were awarded without following proper procurement processes. Year after year, the AG highlighted this troubling phenomenon, but the department made no effort to rectify the situation, as evidenced by its consistently ludicrous irregular-expenditure figures.

Irregular expenditure on dodgy contracts could possibly be forgiven if the department had fulfilled its mandate of delivering decent housing. But that was simply not the case. While Magashule's associates, friends and family stuffed their pockets, the province completely missed its housing targets. Today, thousands of incomplete or poorly built RDP houses are strewn all over the Free State. It is a horrific legacy for a politician who has branded himself as a champion of the poor.

So how did it all begin? Shortly after being sworn in as Free State premier on 6 May 2009, Magashule announced with great fanfare that his administration would build 'bigger and better' houses. These houses would be 50 square metres in size, he promised, an improvement on the 40 square metres previously specified for RDP houses.[6] The man who would help him roll out this new strategy was Mosebenzi Zwane, the freshly appointed MEC for human settlements.[7] While at the time it seemed that Magashule was driven by noble intentions, the benefit of hindsight has led several sources, including current and former department insiders, to view the development in a different light.

When Magashule announced his plan to build bigger houses, the department had already finalised its planning for the following financial year. It had appointed about ninety contractors, who would altogether build roughly 16 000 houses, a former senior staffer told me. However, these builders had been appointed in accordance with the old

PH-094

40-square-metre specifications. The sources I spoke to claim Magashule insisted that the department find new contractors to build the bigger houses, sidelining many of the original contractors.

'The first batch of contractors had already done their bill of quantities based on the old 40-square-metre specifications, and they had signed contracts with the department,' explained the former FSHS official.

With Magashule's new mandate, the department simply failed to honour these contracts. Some of the contractors felt aggrieved enough to take the province to court, but the premier soldiered on. 'Ace told us that people should take him to court if they wanted to; he was going to appoint new contractors,' said my source.

This former official now believes Magashule's call for bigger houses was a ploy to get rid of the original contractors so that a new batch of politically connected businesspeople could benefit from RDP projects. An analysis of the list of new contractors certainly supports this view.

A member of Magashule's erstwhile executive council recalls an even more troubling event. 'Ace called a lot of us together and told us there was going to be this huge series of housing contracts, so we needed to bring "our people" into the mix,' claimed this politician.

According to court papers,[8] in early 2010 the FSHS initiated a fresh tender process based on the new specifications. When the tender closed in April, the department had received bids from 361 contractors. However, amid all the uncertainty over the new specifications, the department was unable to award any contracts before the tender's validity period lapsed. At the end of July, the department's bid adjudication committee met to discuss the contracts.

At this stage, the FSHS was facing disaster. It was already midway into the second quarter of the financial year, and the department had

spent virtually none of its allocation from the national fiscus. If the province could not spend its money, the new premier's administration would come under serious fire from the national government, which could lay claim to any unspent money the province had received through conditional grants. An affidavit filed in court explains: 'If a conditional allocation has not been spent by the end of the financial year, it reverts to and must be repaid to the National Revenue Fund, unless the National Treasury is satisfied that the unspent allocation has been committed to identifiable projects.'[9]

Over and above the R1.3 billion the department had received from National Treasury to build 'sustainable human settlements', it had another R120 million that had rolled over from the previous financial year. Magashule risked having R1.42 billion taken away from his province because of the FSHS's inability to spend its allocation.

'If you don't build houses and spend money during the first two quarters of the financial year, it is pretty much a lost cause,' explained another former FSHS staffer. 'December and January are known as dead months in the construction sector because of the holidays, so you're not going to catch up during that time.'

As the tender had now lapsed, the department seemingly had no way to appoint a large group of contractors in a short space of time so that it could spend its budget. At the July meeting, the bid adjudication committee therefore resolved to cancel the tender and instead draw up a database of service providers made up of 'but not limited to' those who had submitted bids for the lapsed tender.[10] The database could therefore include companies that had not even submitted bids in the first round.

This was not the only problem. Of the 361 companies that did submit

bids, 252 either had bid compliance issues, such as not possessing a valid tax clearance certificate, or had failed to 'meet the minimum functionality threshold'.[11] In other words, they were simply not capable of delivering on large projects. Despite these shortcomings, the department loaded all 361 companies onto its database, along with a few that had not even tendered. Many of them would go on to clinch lucrative contracts to build RDP houses.

Explaining how fraught the process was, one former department official claimed Magashule was the central figure in the saga. 'We were asked to load batches of new companies onto the database, but many of them didn't even have proper NHBRC [National Home Builders Registration Council] papers or the correct CIDB [Construction Industry Development Board] grading, and many of these companies' finances weren't in order,' this source said. 'The technical committee raised these compliance issues with the department's bosses, but they were ignored.' The source alleged that the head of department, Mpho Mokoena, made it clear where his orders were coming from: 'Mokoena told us that Ace had instructed him to work with these people [the new contractors who were found to be non-compliant], that we needed to help them become compliant.'

There were also more overt signs of Magashule's early meddling in the department's affairs. In 2009, he launched his now infamous Operation Hlasela (Operation Attack), supposedly aimed at eradicating poverty and improving service delivery in all spheres of government. But critics say Operation Hlasela was abused for party-political purposes.[12] Indeed, the public protector would later confirm that it 'conflated' the functions of the provincial government with the interests of the ANC.[13]

PH-097

Through Operation Hlasela, which was run out of the premier's office, Magashule exerted control over departments like the FSHS, whose 2016/17 annual report contains a vague explanation of the programme: 'This [Operation Hlasela] is a specific provincial programme focusing on integrated service delivery. All the department's activities are coordinated to ensure integrated human settlements.'[14]

But back to the RDP houses. By October, the FSHS was still woefully behind on its expenditure targets, even after appointing new companies from its dubious database. Tokyo Sexwale, the national minister of human settlements, notified the department that it had spent less than 10 per cent of its allocation.[15]

Losing the unspent money to national government was only one concern. If this were to happen, the FSHS also risked losing out on future grants from the national budget. 'Typically, where a province has failed to spend its conditional allocation, (e.g. for a housing or education project) … the funds will in future years be allocated to other provinces which have a good track record in spending on the relevant housing or education project,' the aforementioned court affidavit explains.[16]

Having more than R1 billion taken away from the provincial government would also have put lethal political ammunition in the hands of Magashule's enemies. They would have been able to accuse his administration of incompetence and maladministration barely a quarter of the way into his first term as premier.

One such political foe was Sexwale. The national housing minister had played a key role in helping Jacob Zuma become ANC president at the Polokwane conference in 2007. For this, Sexwale had been rewarded with a place in Zuma's cabinet. But by 2010, the tectonic

plates beneath the perpetually divided ruling party were moving once again. The ANC's 2012 national conference lay in the not-too-distant future, and Sexwale was already being associated with campaigns and factions that sought to unseat Zuma and his allies.[17] 'Sexwale wanted Ace to fail. He wanted the Free State to pay back the money it couldn't spend to make Ace look weak and incapable,' said a source with insight into the Free State's RDP debacle.

To avoid any embarrassment or political damage, the department had to spend its money as quickly as it could. To this end, it developed an expenditure recovery plan (ERP) to fast-track payments to a new batch of contractors.[18] The ERP was, it seems, masterminded by Magashule's office and enforced by Zwane, but neither man would ever be held accountable for the financial disaster that followed.

With the initiation of the ERP, the money sluices were now well and truly open in the Free State. This sudden profligacy attracted all manner of connected contractors, some of them closely linked to Magashule. One was Rachelle Els, a businesswoman and, according to several sources, a 'close friend' from his hometown. Most concerningly, Els and Magashule were once business partners, or at least intended to be. Company records list Magashule and Els as co-directors in an entity called National Pride Trading 456, which was established in mid-2007, about two years before Magashule became premier. It has since been deregistered. A subsequent chapter details the contracts awarded to Els.

'Ace literally ensured that people got allocated RDP projects,' said one former FSHS insider. 'He would meet with someone like Rachelle Els over the weekend, then on the following Monday we were told that we needed to award 50 or 100 houses to Els's company.'

Several FSHS sources told me there were 'zero tender processes' followed for any of these contracts. They claimed that, through Operation Hlasela, Magashule would hand-pick contractors like Els and ensure that their companies were given RDP contracts. In later court proceedings, the department itself would label the contracts signed in late 2010 and early 2011 a 'fraudulent scheme'.[19]

When the national department and National Treasury got wind of the FSHS's radical expenditure drive, they warned that the ERP was a bad idea. Their main concerns were that the department intended making large advance payments to companies before any work had been done and that the new contracts were signed without following proper procurement processes. They urged the FSHS not to proceed with the ERP, but it pressed ahead anyway.[20]

Between November 2010 and March 2011, the final months of the financial year, the FSHS hastily splurged more than R1 billion, or 90 per cent of its entire budget, on payments to companies appointed for new RDP projects. These projects, awarded to more than 100 contractors, were supposed to have delivered nearly 15 000 houses.[21] Together with contracts signed earlier in 2010, the department now had to deliver around 21 000 houses at a cost of just under R1.5 billion.[22] It was a massive undertaking, and it would soon become evident that the department had bitten off more than it could chew.

The plan could have worked if the department had been capable of monitoring the rapid increase in expenditure. However, what ended up happening was that the FSHS simply emptied its coffers at an alarming rate without putting in place the necessary checks and balances to ensure that the new contractors actually delivered. Of the more than R1 billion the department spent in the last five months of the financial

year, over R600 million was paid to materials suppliers,[23] and about R500 million was paid to building contractors.

According to one of my sources, the ERP was not necessarily a bad idea. Some of the materials suppliers, such as brick manufacturers, required advance payments to keep operating during the weeks in December and January when they would ordinarily have closed shop. The problem was that the department was completely incapable of monitoring the situation to determine which of the materials suppliers had delivered their goods and which of the contractors were building their houses.

When FSHS inspectors did go out to select sites, they found that some of the contractors and materials suppliers had been cheating to increase their profit margins. 'The contracts with the department stipulate that houses need to be built with SABS [South African Bureau of Standards]-approved materials,' my source told me. 'But either the contractors or the materials suppliers, or both, were cutting corners by using cheaper, low-quality materials. That is why some houses in the province started falling apart after two years.' In some instances, contractors had run out of money halfway through their projects. Others had simply not built any houses whatsoever.

At the end of the 2010/11 financial year, after the aggressive expenditure drive had come to a close, the FSHS had still failed to spend R260 million. This money was subsequently reapportioned by national government.[24] It did not reflect well on Magashule's administration, but it was a hell of a lot better than having to pay back more than R1 billion.

From the perspective of the province's would-be recipients of low-cost housing, however, there was little cause for celebration. Some

communities witnessed RDP projects grinding to a halt right in front of their eyes as the inexperienced contractors started running into financial trouble. ‘There were young, new contractors who had never built a single house before,’ one former FSHS official said. ‘Now they suddenly had a R17-million contract to build 200 houses. Some of them took their first payments from the department and bought fancy cars. Others went to the Durban July and partied like there was no tomorrow.’

Some department staffers knew that the situation would inevitably explode into the open. The first sign of trouble came in early 2011, before the financial year-end. In February, Magashule reshuffled his executive council. He sent Zwane to the Department of Agriculture and Rural Development. Mamiki Qabathe, who would later become the speaker of the provincial legislature, replaced Zwane at human settlements.[25]

The move could be interpreted in a variety of ways. One source, a former Magashule ally, said the premier was angry with Zwane because of the R260 million in unspent housing money that the province had lost out on. But perhaps that had merely provided Magashule with an excuse to move Zwane to a department in which his friends from Saxonwold, the Guptas, would soon require a man on the inside. After all, the infamous Vrede dairy project would be initiated in 2012, not long after Zwane became MEC for agriculture, as described in Chapter 14. More likely, however, is that Magashule needed to parachute his henchmen out of the FSHS before any probes into the housing contracts commenced.

Sources familiar with the saga revealed some astonishing information that seems to support this theory. When Zwane left human settlements

for agriculture, he took with him two of the department's most senior financial officials, Seipati Dlamini, the chief financial officer for the cooperative governance and traditional affairs segment of the department, and Mmuso Tsoametsi, the CFO for human settlements.

Dlamini became CFO at agriculture under Zwane, where she got herself tangled up in the Vrede dairy mess. She was arrested and charged over the matter along with agriculture HOD Peter Thabethe in early 2018.[26] Tsoametsi became a deputy director-general at agriculture.[27]

Mpho Mokoena, the HOD for human settlements at the time of the R1-billion spending spree, was also quietly moved to another job. He became head of human settlements at the Mangaung metro municipality.

Sources close to the matter say those four officials – Zwane, Dlamini, Tsoametsi and Mokoena – should have answered for the debacle at the FSHS. 'They were the ones who were getting the instructions from higher up to pay the companies and they were the ones who had the power inside the department to make sure the payments went through,' said one former insider. 'There is no way that a provincial department can spend R1 billion without the approval or involvement of its MEC, HOD and financial heads.'

The FSHS's inability to build houses, meanwhile, was starting to cause unrest and tension in some parts of the province. One tragic day in April 2011, Andries Tatane, a resident of the eastern Free State town of Ficksburg, was shot dead by police during a violent service-delivery protest. He quickly became a martyr of sorts in the intermittent battle between government authorities and some of the country's poorest communities. One of the issues Tatane and his fellow protesters were

angry about was the shortage of decent housing in their area.[28] PH-103

In July, police were again called in to disperse angry protesters, this time in the eastern Free State township of Tshiame. They too were angry about government's failure to deliver low-cost housing.[29] And in Bethulie, frustrated residents showed a *Sowetan* reporter a site where a contractor had left behind houses without roofs, windows or doors.[30]

In early 2012, Magashule again subjected his executive council to a round of musical chairs. The MEC for economic development, Mxolisi Dukwana, a former Magashule ally, had to go. Dukwana had abandoned the Magashule fold and planned to challenge him for the position of provincial chair as a member of the so-called Regime Change group.[31] Led by Mpho Ramakatsa, the Regime Change faction later protested Magashule's re-election as ANC provincial chair by taking the matter to the courts.[32]

Magashule duly fired Dukwana and replaced him with Mamiki Qabathe.[33] The vacant job at human settlements was then given to Olly Mlamleli, who would remain in that position until she became mayor of Mangaung in late 2016. Mlamleli had been close to Magashule since at least 2008. She had worked for him when he was an MEC in Beatrice Marshoff's administration.[34]

The department also got a new HOD in the form of Nthimotse 'Tim' Mokhesi, a former senior official in the Maluti-a-Phofung local municipality in the eastern Free State. Mokhesi served on the board of directors of Maluti-a-Phofung's water utility, where he rubbed shoulders with fellow director Glen Netshivhodza,[35] a businessman from Parys and a close confidant of Magashule. Two of Netshivhodza's companies were among the scores of contractors who benefited from the big RDP splurge of 2010.

Several sources, including department insiders and other government officials, former Magashule allies and some FSHS contractors, all say Mokhesi became the premier's right-hand man in the department. Under Mlamleli and Mokhesi's stewardship, the FSHS would become the site of even more egregious looting involving Magashule, his associates and his direct family.

But first they had to help clean up the fallout from their new department's R1-billion mess. They deftly began tackling the problem in a manner that made it appear as if they truly wanted to get to the bottom of the fiasco.

In July 2012, Mlamleli told the pro-Magashule newspaper *The Weekly* that six department officials linked to the scam had been suspended. The six suspended officials had allegedly made unlawful prepayments to some of the companies involved in the scheme and had manipulated the department's individual subsidy system to make sure the companies got paid, according to the news report. Department officials had also done very few inspections to make sure that the contractors were actually building houses. In her 'exclusive' interview with the publication, Mlamleli vowed to 'root out corruption' at her new posting.[36] In a subsequent annual report, the department explained that there had been 'collusion between employees and suppliers and overriding of internal controls and the department's information systems'.[37]

But according to my sources, the six suspended officials were just scapegoats. 'Those are all people on the level of director or chief director,' said one. 'They reported to the MEC, the HOD and the CFOs, so it made no sense that they alone were made out to be the masterminds. Some of them may have been guilty of some

wrongdoing, but they couldn't be held accountable alone.' But Zwane and Mokoena, former MEC and HOD respectively, were of course safely tucked away in other spheres of government by then. So too was Dlamini, the former CFO.

Around this time, the auditor-general also probed the debacle and confirmed that houses that had been uploaded onto the department's housing subsidy system (HSS) could not be physically verified.[38] In other words, some of the contractors had been paid for houses that were never built. Others had started their respective projects but then abandoned them, leaving scores of unfinished houses all over the Free State.[39]

Magashule and Mlamleli met with senior department officials in April 2012 'to discuss the fact that contractors appointed to construct the … houses were simply not performing', this according to an affidavit to which Mokhesi would later depose.[40] 'At the meeting, it emerged that the contractors' failure to perform under their contracts was largely caused by the fact that materials had not been delivered to them by the suppliers,' Mokhesi stated.

The FSHS, it seemed, had decided at an early stage that it would apportion most of the blame to the suppliers of building materials, despite the fact that the department's primary contractual relationship had been with the builders. This would create an opportunity for Magashule's associates and other politically connected beneficiaries to escape scrutiny and avoid being held financially accountable.

The department subsequently appointed Open Water, a private forensic auditing firm, to probe the matter. It also appointed two private engineering firms to determine the scale of the wastage. Considering the earlier probe by the AG and the involvement of the

National Urban Reconstruction and Housing Agency (NURCHA), an arm of the national Department of Human Settlements, there was no shortage of investigations into the saga.

The Special Investigating Unit had also been on the scene since early 2012. While briefing Parliament's portfolio committee on housing in August 2012, Sexwale said that the SIU had been tasked with probing the Free State contracts under 'Special Presidential Proclamation No. 35',[41] which called for a wide-ranging investigation into fraud and corruption involving the national and provincial housing departments and local authorities.[42] Sexwale also told the committee that the Free State's housing debacle involved irregular expenditure of at least R500 million.[43] Later, in court filings, the department itself indicated that about R500 million of taxpayers' money had been flushed down the toilet.[44]

'No stone will be left unturned in our drive to arrive at the centre of any housing related questionable financial misconduct,' Sexwale vowed before the committee. 'This is disheartening because this is poor people's money. I will be taking this issue to the Cabinet.'[45] He even suggested that the provincial department could be placed under administration in accordance with Section 100 of the Constitution. With only months to go before the ANC convened in Mangaung for its national conference, Sexwale's statement was a barely veiled attack on Magashule and his provincial administration.

But it would be his final say on the matter. Sexwale's bid to become the ANC's deputy president at the party's fifty-third national conference was a complete failure. He did not even make it onto the eighty-member NEC.[46] Zuma axed him as housing minister not long thereafter.[47]

PH-107

Fall guys and fat cats

Magashule must have been relieved that Sexwale was no longer around to scrutinise his province's housing projects.

In 2013, Olly Mlamleli and Tim Mokhesi began legal proceedings to try to recover a significant chunk of the misspent fortune. The FSHS served summonses on 22 of the more than 100 companies involved in the saga. These companies, mostly materials suppliers, had altogether received R631 million throughout the 2010/11 and 2011/12 financial years.[1] In court papers, the department maintained that the suppliers had benefited from 'unjust enrichment', and it wanted them to pay back the money.[2]

It was a curious strategy. Going after the materials suppliers was all well and good if the department could prove that they received money without supplying any materials. But it made no sense that the department chose not to pursue the contractors as well. After all, the contractors had received more than R500 million among them, and the department was already on record saying that these companies were at least as guilty as the materials suppliers when it came to the non-delivery of houses.

Mokhesi's later affidavit summed up the scale of the fiasco: When the department awarded the construction contracts, it split particular housing sites amongst different contractors – for example, several contractors would be appointed to build houses in a particular township, with each contractor responsible for a particular number of houses in that township.

> It was therefore difficult, if indeed possible at all, to determine which contractor had been responsible for what. The difficulties were exacerbated because, in a single township, there were various results – some houses may be completed; others partly completed; others not built at all or barely started; and where construction work had been done, it was often faulty.[3]

Mokhesi also bemoaned the fact that none of the contractors or suppliers had kept proper records of their projects, as stipulated in their agreements with the department. 'The contractors' paperwork was either totally inadequate or simply did not exist,' he said. 'Nor have the material suppliers themselves ever provided proper reports to the department.'

Yet, for some reason, Mokhesi and his department targeted only a select batch of materials suppliers to try to recover some of the money.

The FSHS finally dismissed five of the six suspended officials in June 2015.[4] Other heads would roll later, bringing to eleven the number of officials the department fired. Yet, despite the department's insistence that the officials had been solely responsible for the 'unlawful and fraudulent scheme',[5] it failed to lay criminal charges against any of them.

Mokhesi would later allege that Mokoena, the former HOD, had been 'directly responsible' for the payments.[6] Yet he was not among those who were dismissed. Instead, Mokoena got a plum job as head of human settlements at the Mangaung metro.[7] Of Zwane, Dlamini and Tsoametsi there was no mention. Corney Twala, another top official, also dodged the bullet of dismissal. He was absorbed by the provincial Department of Social Development, where he became a senior

manager.[8] So, not only did the department fail to lay charges against the alleged culprits, but the province and the local metro also provided some of them with a safety net.

The axed officials, however, were not so lucky. I spoke to one of them. This person provided me with a troubling account of events that preceded their dismissal. This account is supported by documents filed in arbitration proceedings and by corroboration from other sources. The arbitration matter, instituted by five of the dismissed FSHS staffers, was still ongoing at the time of writing.

When Sexwale first became aware of the R1-billion fiasco, he desperately wanted to bring Magashule to book. That is why he insisted that the SIU probe the matter. The unit's investigation formed part of a wider SIU probe into RDP projects in provincial departments and municipalities all over South Africa. Their work on the Free State contracts, however, was allegedly severely hampered and eventually derailed by the involvement of Open Water, the forensic outfit appointed by the department to investigate the matter in mid-2012.

Although the firm was technically contracted by the FSHS, several sources told me that the order to appoint it came from Magashule himself. They maintained that Magashule had a close relationship with Open Water's chairman, Reavell 'Ricky' Nkondo, a former spy boss at the National Intelligence Agency.

The premier's official diary, obtained through a Promotion of Access to Information Act (PAIA) request, confirms that there was contact between Magashule and Nkondo after Open Water was appointed by the FSHS. In one instance, Magashule met Nkondo for a 'private meeting' at Free State House, the premier's official residence, one evening in mid-July 2013.

I asked Peet Pieterse, Open Water's CEO, about his partner's meetings with Magashule. He replied: 'Mr Nkondo cannot recall the private meeting with Mr. Magashule but agrees that he did meet with the Premier on occasion. We generally briefed the Premier on investigations during ExCo meetings, in the same manner and meetings where other forensic auditors provided feedback on investigations.' The purpose of the 'private meeting' at Magashule's residence therefore remains a mystery.

A member of one of Magashule's earlier executive councils told me Open Water had been brought into the Free State by Magashule shortly after he became premier in 2009. 'The province needed to verify its payroll system, and Ace told us to use Open Water,' said the source. From that point onwards, the firm acted like 'cleaners' when it came to the Magashule administration's shadiest contracts, this person alleged. 'They covered up a lot of things, but they also did some good work,' claimed the source.

Pieterse denied that they were pulled into the Free State by Magashule. The firm was previously known as Ramathe Fivaz and had been present in the province since 2001, he said. He took exception to Open Water being referred to as Magashule's 'cleaners'. In his defence of the firm, he made a rather curious remark. 'We were probably rather Mr Magashule's henchmen than cleaners and we were not well liked as our appointment resulted in employees and office bearers being dismissed and/or criminally charged,' Pieterse contended in a written response. He said he could 'categorically' state that Magashule 'never once asked [Open Water] to manipulate any findings or omit any evidence from [their] reports'.

But the perceptions of an unusually close relationship between the

firm and the then premier prevailed. One of my sources told me Open Water's chairman, Nkondo, married Rooksana Moola, a staffer in Magashule's administration, after the firm started working in the Free State.

Pieterse insisted that this presented no problems whatsoever. 'Mr. Magashule's administration was vast and she [Moola] did not work in close proximity to Mr. Magashule, or even in his office, and therefore the insinuation that they married as a consequence of Mr. Nkondo being that close to Mr. Magashule is not only mischievous but devoid of fact or truth.'

If there is anything to say about Nkondo, it is that his career as a government spook was seemingly eventful. In 1997, then Pan Africanist Congress (PAC) politician Patricia de Lille included Nkondo's name on a list of former ANC underground operatives who had allegedly acted as double agents for the old apartheid government.[9] The ANC denied the existence of such a list. His name also surfaced during the 2003 Hefer Commission of Inquiry into allegations that NIA spooks had spied on National Director of Public Prosecutions (NDPP) Bulelani Ngcuka. Nkondo was portrayed as a functionary of the Zuma camp in the highly politicised 'spy wars' of the early 2000s.[10]

After Open Water's appointment by the FSHS, the SIU's Free State branch was apparently strong-armed out of the probe.

A source in the law-enforcement environment with insight into the matter claimed that at one point the SIU was asked to stop its investigation. 'The SIU was told to stop working on the Free State contracts,' he told me. 'I don't know where that order came from, but it must have been from a very senior political office.'

Another source, an SIU insider, said Open Water effectively blocked

the SIU's investigative efforts. 'We were told by the department that Open Water took computers, documents and other records,' this source said. 'When we asked for certain documents, Open Water would tell us they didn't have it.'

Contrary to normal investigative procedure, Open Water also allegedly failed to compile a record of what exactly they had taken from the department. This added to the SIU's headaches. 'When we asked for a certain document or contract and Open Water said they didn't have it, there was no record of what they had taken to determine if they were being honest with us,' said my SIU source.

Most alarmingly, the Open Water team allegedly took some documents related to the R1-billion splurge to Magashule's office. 'All the documents were taken to Ace's office on the fourth floor [of the Lebohang Building in downtown Bloemfontein],' claimed one current FSHS insider.

Pieterse denied all of this. 'We kept detailed inventories of each document removed from the department as well as the documentation and electronic data returned.' He said he knew nothing about documents that may have been taken to Magashule's office. 'The investigation relied on a vast number of records and to remove certain records to "take" to the Office of the Premier would serve no purpose to influence the outcome of the investigation,' Pieterse maintained.

The Open Water CEO said the firm had 'never obstructed or prevented any investigative agency in performing their work and has always and will always co-operate with such agencies, which was also the situation in the FS housing matter.'

However, the tone of his response made it clear that there had indeed been friction between Open Water and the SIU. 'The SIU was

appointed approximately a year before Open Water was appointed and one would expect that after such an extended period they would have collected the documentation required. When we were appointed they made little progress,' said Pieterse.

An SIU investigator had asked Open Water for the firm's mandate for its investigation, but Open Water refused to comply. 'I respectfully advised him that he held no proclamation to subpoena me for the information, whereafter no further requests for any documentation were received from the SIU,' said Pieterse.

The strangest thing about Pieterse's response was that he tried to convince me that Open Water and the SIU had been tasked to probe entirely different matters. 'My understanding was that the SIU was mandated to investigate the development and delivery of low-cost housing at the time for the period ended July 2010.' The Free State's R1-billion RDP splurge only occurred at the end of that year. 'It is therefore obvious that we investigated different matters and therefore we could not have restricted the SIU or any other law enforcement agency in performing their work,' maintained Pieterse.

But it wasn't 'obvious' at all.

The SIU, in a formal response, made it clear that it had probed the same advance payments Open Water investigated. 'The investigation pertaining to the unauthorised payments of advances by the Free State Department of Human Settlement[s] regarding the 2010/2011 and 2011/2012 financial years is finalised. The findings and recommendations are contained in a report addressed to the Office of Presidency, who acknowledged receipt of the said report on 2 October 2015,' the SIU said in a letter it sent me in October 2018.

Even FSHS HOD Tim Mokhesi confirmed the SIU had been on the

scene. 'The prepayments matter relating to material suppliers were investigated by the Special Investigation Unit (SIU),' he said in a written response.

Considering Open Water's alleged meddling, one can't help but wonder how thorough the SIU report was.

The SIU also told me that it had referred three matters to the National Prosecuting Authority for criminal prosecution. The NPA 'in turn referred [the three cases] to the Hawks for finalisation'. But that was more than three years ago. It appears as if these cases were added to the mountain of investigations that ground to a halt once the Hawks got hold of them during Zuma's years in power.

Open Water started its investigation on 19 June 2012 and submitted a preliminary report a mere ten days later. It was on the basis of this report that the department suspended and later dismissed eleven officials.[11]

But Open Water's methodology apparently left much to be desired. My source within the group of axed officials claimed that the investigators did not even bother to interview any of the alleged culprits. 'The Open Water guys came to the department, took our gadgets [computers and other electronic equipment] and then told us to leave the premises,' said the former official. 'They never spoke to us to collect our side of the story.'

The firm and some of its key executives have been accused of employing similar tactics elsewhere. A *Sunday Independent* report from 2017 detailed how an Open Water report had implicated a local logistics company in a supposedly dodgy deal with South African Airways Technical. It had then emerged that Open Water had not interviewed the implicated company's managing director before it

concluded its probe.[12]

PH-115

A 2016 report by amaBhungane highlighted further concerns over forensic work by Pieterse and Open Water, this time involving the Council for Scientific and Industrial Research (CSIR) and its then CEO, Sibusiso Sibisi.[13]

Pieterse's forensic work was also severely criticised by a judge in the Eastern Cape High Court in 2005. A forensic report compiled by Pieterse formed the basis of a fraud case against three senior officials from the Eastern Cape Development Corporation (EDC).[14] Mcebisi Jonas, the EDC's then CEO, was among the accused.[15] The fraud charges were viewed as being part of a political witch-hunt, and Jonas and his co-accused were eventually acquitted.[16] In his ruling, Judge Dayalin Chetty said Pieterse's report showed 'a complete lack of objectivity', was 'severely wanting' and displayed an 'erroneous interpretation of the applicable legislation', according to a *Mail & Guardian* report.[17] The newspaper seemingly directly quoted from the judgment, but Pieterse claimed the publication got it wrong. 'The Eastern Cape matter was my first encounter with the influence of politics and the media on reality,' he told me. 'I have no doubt that in a different time or a different province the outcome of the trial would have been different.'

Meanwhile, after the FSHS officials were suspended, they naturally demanded to see Open Water's report. They wanted to see for themselves how the probe had concluded that they were the guilty parties. 'We wrote to them [Open Water] and asked for the report, but they never got back to us,' claimed one of the axed officials. Some of the suppliers implicated in the FSHS's legal proceedings would later have similar problems, the owner of one such business told me.

Frustrated, the suspended officials turned to the SIU in Bloemfontein. 'We asked the SIU if we could see the Open Water report or any of the documents that supposedly proved we were guilty,' my source explained. 'He told us Open Water took all the department's records.' Even the SIU failed to obtain the Open Water report, my unit source told me. Pieterse claimed the SIU never asked for the Open Water report.

Five of the axed FSHS officials, meanwhile, decided to fight back. They instituted arbitration proceedings against the department in which they challenged the outcome of their internal disciplinary hearing. Their filings[18] laid bare the alleged involvement of Magashule's office and the roles played by Zwane and his fellow department bosses in the most fundamental decisions that led to the R1-billion RDP splurge.

'They [the axed officials] simply fell victim to a modern government contagion – *i.e.* that the powers that be go about their functions in certain ways (whether lawfully or motivated by malfeasance), implement what is decided in higher structures, and when the actions go wrong some subordinate is sacrificed at the altar of the true culprits,' their legal counsel contended.

Drawing on heaps of documents and records, their submission alleged that 'the scheme' was orchestrated by Magashule's office and implemented by the likes of Zwane, Mokoena and Dlamini: 'It cannot be overstated that this entire model and the operation of the scheme … emanates from the office of the Premier and employees in the Department responsible for legal compliance.'

The cornerstone of the ERP, namely the contracts between the FSHS and the various contractors, was in fact sanctioned by Magashule's own office, the axed officials argued. 'The chairperson [of the

disciplinary proceedings] forgot that the State Law Advisors were asked – at the offices of the Premier – to advise on the drafting of the contracts.'

Their counsel added that the ERP 'was thoroughly researched, contracts drafted and the "OK" given by inter alia Mr Tsoametsi, Mr Taka [the FSHS's deputy director for legal services], the State Law Advisor and Mr Bertus Venter at the Premier's office'.

The officials argued that if they had been implicated in an unlawful scheme, it was because they were acting on orders from higher up. 'The applicants never took the decision to implement the advance payment system,' reads their submission. '[This] was introduced through a decision taken by the Member of the Executive Council [Zwane], the Head of the Department [Mokoena] and the Chief Financial Officer [Dlamini].'

As mentioned earlier, these arbitration proceedings are ongoing. But it seems almost certain that Magashule and some of his key henchmen, including Zwane, orchestrated and executed the plan that resulted in the FSHS emptying its coffers in record time.

The court application that included Mokhesi's affidavit was lodged in late 2016. The department sought to have the Bloemfontein High Court review and set aside its contracts with 106 companies: 85 building contractors and 21 materials suppliers. In terms of trying to retrieve some of the misspent money, however, the department instituted action proceedings against just 22 of the companies in an attempt to recover R631 million. Surprisingly, these included all 21 materials suppliers and only one building contractor. The department was clearly targeting the materials suppliers.[19]

One of the owners of a materials supplier from which the department sought to recover money told the *Sunday Times* that the department's legal bid was a 'façade' and a 'smoke screen'. The R1-billion expenditure drive had been marred by fraud, the businessman said. According to him, the department had merely cited the 106 respondents to convince the SIU that it was doing something about the looting. He lamented the fact that the department had chosen to try to recover money from the materials suppliers only, seeing as some of them had delivered the goods for which they had been paid.[20] 'What about those suppliers and contractors who were paid in advance but are not listed as respondents? Why are they being protected?' the businessman wanted to know.

It sounded to me like the department's selective legal bid to recover some of the money was a cover-up. I obtained documents and records pertaining to the department's expenditure during that period and proceeded to analyse them. It was a classic exercise in following the money, and the results were frightening. I began to realise why Magashule may have wanted to take control of the investigative process.

There were several materials suppliers and contractors, who collectively received a fortune as part of the R1-billion ERP, who were seemingly overlooked in the department's legal proceedings. Some of them were closely linked to Magashule. We'll start with a few materials suppliers who managed to slip under the radar.

In 2011, while human settlements agency NURCHA was probing the matter, an email was sent to several companies that had received advance payments for materials. The email, of which I obtained a copy, contained the names of all 21 suppliers against whom the FSHS had

instituted action proceedings to recover the R631 million. However, also included in the email were the names of an additional five companies not mentioned in the department's court filings. These companies had collectively received more than R35 million in 2010/11 alone, according to records from the department's housing subsidy system.

One such supplier was Friedshelf 863. When I looked at its records at the Companies and Intellectual Property Commission (CIPC), I found the name of one of Magashule's oldest and most trusted pals. Hantsi Matseke (née Mayeza), a fellow Parys local whose relationship with Magashule goes back to their Hillbrow days, registered the company in 2007. Its name was later changed to Maono Construction, and it features elsewhere in this book. Matseke also registered a joint venture (JV) with a company called Ubuhlebethu Property Developments in October 2010. In other words, the JV was established just in time for the FSHS's splurge. The JV subsequently scored a contract to build 271 houses in Bohlokong outside Bethlehem. This project was awarded to Matseke and her partner as part of Operation Hlasela, the premier's development programme.

Matseke became chairperson of the Free State Development Corporation in July 2012. As we will see in later chapters, this state-owned entity has been very kind to Magashule's daughter, Thoko Malembe, who also later became Matseke's business partner.

Although the NURCHA email listed Friedshelf 863 as a supplier, the department's HSS refers to the company as a 'contractor/builder'. The HSS shows that Matseke's company received a small fortune from the department. In 2010/11, it was paid just under R6 million. In the following financial year, it received R38 million. By 2014, Friedshelf

863 had pocketed altogether R52 million from the FSHS. The JV, meanwhile, earned just over R23 million for the Bohlokong project. PH-120

Matseke said her company should not have been included in the email regarding NURCHA's probe into the advance payments. She said Friedshelf 863 had been paid as both a supplier and contractor, but didn't receive any money in advance. Her company was not 'implicated by the findings of the investigation', she said.

The HSS suggests that Friedshelf 863 and its JV partner left behind incomplete houses at the Bohlokong project. Matseke said the JV finished all but seven of the houses it was supposed to deliver. This was due to 'beneficiary management challenges'.

After being rebranded as Maono Construction, Matseke's firm began to soar in the Free State. Its contracts from the FSHS alone in the period after 2013 were worth more than R150 million, according to the HSS. In total, Maono bagged more than R500 million in contracts from the FSHS and other departments in Magashule's provincial government.

Matseke did not take kindly to my questions about her relationship with Magashule. 'I find this line of question[ing] unacceptable, extremely offensive and hurtful as it creates an innuendo that my companies get contracts as a result of certain perceived relationships. In short, this is degrading, sexist and undermining to black business women in this country,' she said. She denied that Magashule played a role in contracts awarded to her companies.

Despite Friedshelf 863 having featured in the NURCHA probe, as suggested by the leaked email, the department chose not to list the company in its court bid, thus shielding Magashule's chum. Worse still, there were suppliers who received money in the 2010/11 splurge that

did not even feature in the NURCHA investigation, let alone the department's later legal proceedings. The payments to these companies are reflected in the HSS.

One such company that drew my attention was Robs Bricks. The database showed that it had received exactly R7 million, a figure that stood out like a sore thumb among the hundreds of payments. It is highly unlikely that any supplier would have provided materials valued at such a precisely round figure.

The company's CIPC records confirmed that my suspicions were justified. Like the JV between Friedshelf 863 and Ubuhlebethu, Robs Bricks had been registered just in time for the department's 2010/11 spending spree. And its sole director was Mohlouoa 'Blacky' Seoe, one of Magashule's former business partners.

Seoe has another company – Robs Investment Holdings – which benefited from the FSHS's largesse to a much greater extent than Robs Bricks. What's more, the HSS shows that its success correlates exactly with Magashule's tenure as premier. Between 2010 and 2017, Robs Investment Holdings netted almost R90 million from the department. Like its sister entity, it was not mentioned in the FSHS's court application.

A 2013 progress report on some of the department's projects sheds light on Robs Investment Holdings' poor performance. During the R1-billion splurge of 2010, Seoe's company clinched contracts to build 400 houses in the former homeland of QwaQwa and in the town of Kestell. By February 2013, it had completed only 187 units. According to the report, Robs Investment Holdings had experienced problems with sourcing materials. At the Kestell site, some of the would-be beneficiaries had become so tired of waiting that they had started to

construct their own houses.[21]

Like Matseke, Seoe is also linked to Magashule and his daughter Thoko through business dealings. Magashule was once a director in Sambal Investments, another of Seoe's companies. And I identified at least one property transaction between one of Thoko's trusts and a company owned by Seoe. This deal, incidentally, went down in Kestell. Moreover, when I was working on an investigative piece for *News24* in 2017, I found CCTV footage showing Magashule, Thoko and Seoe, along with some others, inspecting a Shell fuel station in QwaQwa. Thoko later scored this property in a dodgy deal involving the FDC, the entity chaired by fellow RDP contractor Hantsi Matseke.[22]

One of the FSHS insiders I spoke to said the department deliberately excluded Seoe's companies from the court application. 'He got advance payments and his two projects were never finished, but he didn't get sued due to his close proximity to Magashule and Mokhesi,' said this source.

Peet Pieterse, meanwhile, denied that Open Water had overlooked companies owned by Matseke and Seoe. Robs Investment Holdings and Friedshelf 863 featured in the Open Water report, he insisted. However, I had asked him about Robs Bricks, not Robs Investment Holdings, seeing as the prior company had received the strangely round figure of exactly R7 million for materials. Pieterse did not indicate whether this entity featured in the Open Water report.

I asked Pieterse why some of the entities included in the Open Water report had apparently been excluded from the FSHS's legal proceedings against contractors and materials suppliers. He said Open Water did not have a say in determining who the FSHS ended up suing.

'It may be that the entities did fulfil their obligations in terms of their

agreement[s] with the Department by constructing all the houses, which may therefore cause the advance payments to be of no consequence in civil proceedings had the Department received value for money in terms of the enrichment principal,' said Pieterse.

A proper analysis of the HSS reveals scores more companies with strong political connections, many of them owned by people close to Magashule's inner circle.

The entity with perhaps the funniest name must be Mob Business, a closed corporation that was registered in 2002 by Moreki Moroka, the wife of lawyer and long-time Magashule associate Kenosi Moroka. Magashule and Kenosi were previously co-directors in two companies.

A 2009 *Mail & Guardian* report detailed how Kenosi Moroka allegedly tried to extract a R2-million bribe from a businessman who needed the approval of the Free State Gambling Board for a deal involving the transfer of shares in a casino company. It was alleged that the lawyer had acted on Magashule's behalf.[23]

Sources who attended gatherings or meetings with Magashule alleged that Moroka is something of a benefactor to the former premier. 'I've been to meetings with Ace and some of his associates where we racked up large bills,' said one individual. 'Kenosi would sometimes pull out big wads of cash and settle the bill.' Moroka strongly denied this. 'Our client has never been in any meeting where Mr Magashule and some of his political allies held meetings where our client had to settle restaurant bills,' his law firm said on his behalf.

Moroka should also be familiar with Mokhesi, under whose watch the FSHS drove legal proceedings in relation to the R1-billion RDP splurge. Moroka and Mokhesi have served together on the board of Centlec (SOC) Ltd, the local state-owned power distributor, since

2013.[24] Incidentally, Seoe has also done a stint as a Centlec director.[25]

Moreki Moroka seemingly hit the jackpot when Magashule became premier in 2009. Mob Business pocketed more than R50 million in revenue from the FSHS between 2009 and 2018, according to the HSS. This included a payment of just over R5 million in 2010/11 to build houses in Bloemfontein. In that same year, Moreki and Mosidi Motsemme, the mother of two of Magashule's children, bought properties within walking distance of each other in the same upmarket residential estate on the outskirts of Bloemfontein. Motsemme is known in Free State ANC circles as Magashule's 'Bloemfontein wife'.

Moroka denied that her business's successes could be attributed to perceived political connections. 'The libellous disinformation that seeks to link the operations of Mob Business to the tenure of Mr Magashule as the Premier of the Free State Province are, to say the least, preposterous and malicious,' said her lawyers.

According to the FSHS's 2013 progress report, Mob Business left behind 100 unfinished houses in Bloemfontein. 'Contractor not on site for four months,' reads the report. 'Recommend to terminate.'[26] Although Mob Business was listed as a respondent in the FSHS court bid, it was not among the companies against which the department instituted action proceedings to recover money.

Moreki Moroka insisted that her company did finish all its houses in Bloemfontein. 'As further testimony to [the] absence of malperformance, the Department duly paid the retention fee to our client, which would not be paid in the event [that] there was defective performance present,' claimed her lawyers.

10

Rewarding friends and punishing foes

While poring over Tim Mokhesi's affidavit and the FSHS's court application, I noticed something interesting.

As mentioned previously, there were 106 respondents in the department's 2016 court application, including the 22 companies from which the department sought to recover R631 million. Of the 106 respondents, 93 are closed corporations or private companies. The remaining respondents are natural persons listed in their capacity as trustees of trusts that received money from the department.

Relying on the court papers, the *Sunday Times* had revealed in January 2017 that former SABC chief operating officer Hlaudi Motsoeneng and the wife of sport minister Fikile Mbalula were among those listed as respondents.[1] Motsoeneng and Mbalula, who would become minister of police in March of that year, both hailed from the Free State. Motsoeneng and Mbalula's wife, Nozuko, were both members of a trust that apparently scored contracts worth about R38 million to build 450 houses in Virginia and Bloemfontein respectively, the newspaper reported. But the houses were never finished.

When asked for comment, Motsoeneng simply stated that he had 'no interest' in the issue. Nozuko denied that she had been involved. 'I'm

very angry,' she told the *Daily News*. 'I'm seeking legal advice on how to clear my name in this regard. I'm being labelled a fraudster. I feel my name has been abused.'[2]

PH-126

The inclusion of Nozuko Mbalula's name in the court application is interesting in light of her husband's strained relationship with Magashule. The beef goes back to 2012, when Mbalula aligned himself with the Free State ANC's Regime Change group. This faction sought first to unseat Magashule as provincial chair before backing the anti-Zuma slate at the Mangaung conference at the end of that year.[3] The group ultimately failed, and the movement fizzled out in 2013.

Nevertheless, the hostility between Magashule and Mbalula continued to build well into 2017. Not long after his move to the police portfolio, Mbalula took aim at Magashule in one of his famously belligerent tweets. 'Ace Magashule is a definite no no no, the man will finish what is remaining of our movement. He will kill it,' Mbalula tweeted in June 2017, after it became clear that the premier would run for the position of ANC secretary-general at the end of that year. Mbalula's animosity was probably heightened by the recent court action implicating his wife in the Free State housing scandal.

I have always suspected that the inclusion of Nozuko Mbalula's name in the court papers was an attempt by the Magashule administration to settle a political score with her husband. My theory is supported by further compelling indications that the department used its court application to help fight Magashule's battles.

Of the 93 corporate structures listed as respondents, the department included the names of the managers or owners of only four. Of the four people named, three can be linked to political squabbles with Magashule. While the four entities are listed as respondents, they are,

however, not among the companies from which the department sought to recover money.

Listed next to one another, as the 17th and 18th respondents respectively, are Clear Creek Trading 115 and Makana Women Construction. According to the court papers, Clear Creek Trading is in the 'care of Petrus Zanemvula Matosa' and Makana Women Construction is in the 'care of Mpho Ramakatsa'. According to the HSS, Clear Creek Trading received more than R2 million in 2011. Coincidentally, Matosa and a few co-directors registered the company in June 2009, a month after Magashule was sworn in as premier. Makana Women Construction has to date earned more than R20 million from the FSHS. This includes payments totalling almost R10 million during the time of the department's big expenditure drive.

What is relevant to this narrative is that Matosa and Ramakatsa both crossed swords with Magashule around this time.

Matosa, a former ANC provincial chairperson and erstwhile member of Magashule's inner circle, had begun to drift away from his former ally in around 2009. Ramakatsa was a leader of the so-called Regime Change group, which locked horns with the Magashule faction in an acrimonious battle for power in the province. Ramakatsa had also orchestrated the court battle that ended in an embarrassing legal lashing for the Magashule camp in late 2012. The Constitutional Court had ruled that the Free State's provincial elective conference held in mid-2012, and where Magashule was re-elected as chairperson, had been fraught with irregularities. The Provincial Executive Committee had therefore been elected unlawfully, the court found.[4]

As a result, the national leadership had dissolved the PEC and scheduled another elective conference for May 2013.[5] It looked as if

Ramakatsa was going to challenge Magashule for the position of provincial boss, with Matosa on his slate vying for the position of secretary.[6] But the Regime Change group suffered a major blow when Ramakatsa's branch was barred from participating in the conference.[7]

Ramakatsa later claimed that the second conference, which again re-elected Magashule and his cohorts, was as riddled with irregularities as the previous one.[8] But instead of mounting a fresh legal challenge, Ramakatsa joined the Economic Freedom Fighters (EFF). Matosa, for his part, faded into political oblivion. As far as their companies were concerned, someone behind the scenes ensured that the provincial government's money taps were closed to them for good. Makana Women Construction and Clear Creek Trading received their last payments from the FSHS in the 2012/13 financial year, according to the HSS.

I had a chat with Matosa in late 2018. He said the RDP splurge amounted to 'fiscal dumping', but that the companies targeted in Mokhesi's court application were 'dolphins' while the 'sharks' were let off the hook. As for his own company, Matosa maintained that he was only paid for work that he had completed and for which he had submitted claims. 'Clear Creek got a contract to build 200 houses in Brandfort,' he told me. 'It rained heavily for about four months during that time, so we could only finish about 100 houses before the contract period lapsed. But we were only paid for the houses we completed.'

He felt that he had been targeted in the lawsuit for political reasons. 'They tried to destroy me and Mbalula, through his wife, by listing us in the court papers,' he said.

The third significant person listed in the department's court application is Maggie Nthatisi, wife of Gregory Nthatisi, a former

Umkhonto we Sizwe member who later served alongside Magashule in the 1994 provincial cabinet appointed by Mosiuoa Lekota.[9] Sources familiar with Free State politics told me that Nthatisi played a crucial role in helping Magashule become provincial chair at the 2002 elective conference.

In the 2000s, the Nthatisis started doing brisk business with the Free State government, especially in the low-cost housing sector. The HSS shows that four companies managed by or linked to them have over the years earned revenue of about R400 million from the FSHS. This includes payments of about R23 million in 2010/11, the year in which the department's 'fraudulent scheme' was rolled out.

But, like Mbalula, Gregory Nthatisi was associated with the 2012 Regime Change movement, with the de facto mouthpiece for the Magashule administration, *The Weekly*, going so far as to call him the 'face' of the campaign. For someone who had so richly benefited from government contracts, Nthatisi had some harsh words for the Magashule regime. 'This move … in its nature is aimed at stopping the abuse of power, patronage, corrupt practices at the level of the ANC and state power,' he said.[10]

Nthatisi's 'betrayal' coincided with a dramatic turn in fortune for his and his wife's low-cost housing empire. The FSHS's financial data perfectly encapsulates how their businesses suffered the same fate as those of Matosa and Ramakatsa in the wake of the unsuccessful attempt to oust Magashule and his allies.

In the 2011/12 financial year, just before the Regime Change challengers mounted their attack, the four Nthatisi businesses earned a healthy R25 million in revenue from the FSHS. But by the following financial year, their revenue was down to just under R4 million. And in

2014, the companies collectively earned a paltry R800 000. After that, they did not receive a single cent from the department ever again.

The data correlates with anecdotal evidence that Magashule abused his power as premier to financially reward politically connected contractors who stayed loyal to him, while punishing those who somehow betrayed him. 'If Ace felt that you had stabbed him in the back, he made sure that you never again got contracts from whichever department you had been working with,' said a former close associate of Magashule.

Mokhesi said it was 'not true' that he and the FSHS had used the court application to target Magashule's political foes.

Another major beneficiary of low-cost housing contracts in the Magashule era is soccer-club owner turned construction mogul Mike Mokoena, whose company Tshwara Thebe Construction, or TTC, received contracts from the FSHS worth R310 million between 2012 and 2018. While TTC was one of the 106 respondents in the department's court application, it was not sued to return some of its earnings.

Mokoena is best known as the owner and chairman of the Free State Stars, a professional soccer team based in Bethlehem in the eastern Free State. His career as a tenderpreneur appears to have taken off in 2002, when a collection of companies he co-owned with various family members clinched tenders from the provincial departments of social welfare and education to deliver food parcels, textbooks and stationery.[11]

Mokoena has no qualms about being labelled a tenderpreneur. 'My life is to tender,' he told the *Sunday Times* in 2010. 'I apply for tenders,

that's my lifestyle. I've got guys dealing with tenders full time. I'm not ashamed to say that's my lifestyle.'[12]

PH-131

Magashule seemingly viewed himself as the source of the largesse bestowed on companies like TTC, and he apparently demanded reciprocity from the likes of Mokoena.

One source, a member of the Free State business fraternity, attended a gathering of about fifty contractors at Magashule's office in Bloemfontein in early 2014, before that year's general election. Magashule had invited his favourite friends from the business sector to ask them for a special favour. 'Ace told us we needed to make financial contributions to the ANC for the upcoming elections,' this source told me. 'He said the ANC had been good to our companies, and that he would close the money taps if we didn't support the ANC.'

The businesspeople were asked to each pledge an amount. It was reminiscent of the Free State ANC provincial conference in 2008, when Magashule demanded that party members and invited guests donate towards Zuma's legal fees. According to my source at the 2014 gathering, Mokoena was among those who made the largest pledges to the ANC.

Mokoena said he wouldn't comment on 'alleged rumours' and would only respond to 'factual allegations made by identified persons'.

One 'identified person' was willing to discuss allegedly dubious dealings between Mokoena and Magashule. Mxolisi Dukwana, a former Free State MEC, told me Mokoena once 'pledged' to donate R1 million to the ANC. This was before the Regime Change bloc's failed attempt in 2012 to topple Magashule and his allies. As the ruling party's then treasurer in the Free State, Dukwana was tasked with managing and collecting such contributions. 'The money was to be

paid in two instalments of R500 000. The next thing I knew Ace had collected the first R500 000 himself. Mike did later pay the second R500 000 to the ANC, but the money Ace took did not come to the ANC,' alleged Dukwana.

Mokoena strongly denied the allegation. 'The information at your disposal is false and incorrect. I did not pledge the amount of R1 million at any relevant time nor is it true that R500 000 was collected by Mr. Magashule himself or any other person for that matter,' he said.

Dukwana remained resolute. 'If Mr. Mokoena wants to create an impression that I had imagined things about his pledge to the ANC he is making a big mistake.'

Further careful analysis of the companies listed in the FSHS's court papers and on the HSS reveals that the spouses and children of some of Magashule's senior colleagues in the provincial government and the local legislature also benefited from housing contracts. Subsequent progress reports have highlighted problems with the work of each one of these entities.

People First Construction, Moyakhe Trading, Phahama Development Trust and Jore Construction were all listed as respondents in the court application, but were not sued to recover money. Collectively, these companies received payments totalling over R40 million during Magashule's reign as premier. Unlike the entities owned by or linked to Magashule's political enemies, the names of the directors of these businesses are not revealed in the court papers.

CIPC records show that People First Construction's sole director is Tankiso Morule, wife of Playfair Morule, a long-serving Magashule ally. Morule himself was once a director of the company.

Playfair Morule has held several senior political and executive

positions in the Free State, including MEC for finance, and for safety and security. He later became the ANC's chief whip in the provincial legislature under Magashule's stewardship. A guilty conviction on a charge of culpable homicide following a hit-and-run incident did not stop him from becoming the mayor of Bloemfontein in 2008.[13]

In 2013, at the height of the Gupta shadow state's rule over South Africa, Morule was appointed as South Africa's high commissioner to India.[14] And in early 2018, then public enterprises minister and suspected Gupta backer Lynne Brown apparently tried to have Morule appointed as chairperson of Eskom.[15]

Morule's wife, meanwhile, has reaped the benefits of being a building contractor employed by the Free State provincial government. People First has received almost R140 million from the FSHS to date, according to the HSS. The same records suggest that People First is among the contractors guilty of leaving behind incomplete houses. Of the 200 RDP units this company was appointed to build in 2010, 87 were incomplete in 2013, according to one progress report. People First apparently abandoned the project because of delays in getting paid by the department.[16]

Moyanda Mohai, the wife of another former chief whip turned MEC, has also been on the receiving end of lucrative contracts. She is married to Seiso Mohai, who served as Magashule's MEC for finance from 2009 to 2013.[17] Her company, Moyakhe Trading, has to date received more than R18 million from the FSHS, mostly in the period after Magashule became premier.

Moyakhe Trading got a contract to build 300 houses in Bloemfontein in 2010. By 2013, only 132 houses had been completed. A progress report lists 'cashflow problems' among the reasons for the contractor's

inability to complete the project on time.[18]

PH-134

By the look of things, the Free State legislature was the place to be if you wanted your family members to clinch RDP contracts. The husband of the late Mantsheng 'Ouma' Tsopo, a former speaker of the provincial legislature, got in on the action too. Sandile Tsopo is a trustee of the Phahama Development Trust, which over the years earned revenue of about R36 million from the FSHS. This includes payments made during the big splurge of 2010.

Tsopo was convicted in 2007 on fraud charges related to dodgy contracts from the Free State Department of Education, which his late wife once headed.[19] This clearly had no impact on Phahama's ability to score provincial contracts after Magashule took over as premier.

Along with Hlaudi Motsoeneng and Nozuko Mbalula, Sandile Tsopo was one of the few connected individuals exposed by the media in relation to the 2010 splurge. He told *Volksblad* in 2017 that he had been appointed to build 600 houses in Matjhabeng (Welkom), but that he had completed only 200. He claimed that the project ground to a halt after his materials supplier died, and maintained that he had only received payment for work done and for which Phahama had invoiced the department.[20]

Ouma Tsopo's predecessor as speaker, Moeketsi Sesele, was a member of the Free State's pro-Magashule northern faction. His daughter Masedi is the director of Jore Construction, which received payments of more than R10 million for RDP houses between 2010 and 2014. Jore has perhaps the worst performance record of the four entities linked to politicians in the legislature. Appointed to build 400 houses in Thaba 'Nchu near Bloemfontein in 2010, nearly three years later it had completed only 84 units.[21] Most worryingly, the lives of the

occupants of some of these houses were literally in danger. One of the completed houses collapsed in 2013, and inspectors refused to accept a further fourteen finished houses 'due to poor mortar mix'.[22]

Thutela Bogolo Trading Enterprise was also on the receiving end of large RDP contracts. This is the company owned by Rachelle Els, Magashule's buddy from Parys. Thanks to her powerful friend, Els seemingly established a small RDP empire. Thutela Bogolo earned more than R110 million from the FSHS between 2010 and 2017, including R35 million paid out during the department's problematic expenditure drive in 2010, according to the HSS. Els claimed the department's records were incorrect and that her company had received much less than that.

Department records suggest that many of Els's construction contracts came to her directly from Magashule by way of Operation Hlasela, the premier's controversial development programme. Of the more than 1 600 houses she was allocated to build in 2010 in the towns of Kroonstad, Steynsrus, Oranjeville and Koppies, 510 were given to her through Operation Hlasela.

By early 2013, only 240 of the houses allocated to Thutela Bogolo had been finished.[23] Els admitted that it had taken years to complete some of her houses, but she blamed administrative and financial problems at the FSHS for the delays. She was adamant that all of her construction work had been of the highest quality.

As with other RDP contractors, there were rumours of an unusually close bond between Magashule and Els.

The former premier's official diary confirms that there was contact between the two during his incumbency. For example, in August 2011 Els met with Magashule at his office in Bloemfontein. This was right in

the middle of a financial year in which Thutela Bogolo earned R21 million from the FSHS, according to the HSS.

Several sources have claimed that Magashule often visited Els at her home in Parys and sometimes even spent the night. His diary contains details that suggest this may be true. On the weekend of 20 and 21 October 2012, for example, Magashule's diary shows consecutive 'private visit[s]' at 'Roshelle's Place Parys' [*sic*].

Els told me Magashule sometimes spent the night at a guesthouse in Parys owned by her daughter. 'Everyone in Parys knows him, so he needed a place to stay over where people wouldn't be able to bother him,' she said. Magashule apparently paid for his accommodation.

There is also the matter of an overseas trip that Els, Magashule and other Free State officials embarked on in 2010. My sources told me the then premier went to the USA in that year, and that contractors like Els helped foot the bill.

Els admitted that she went to the USA with Magashule. She denied that she had bankrolled the entire trip, but indicated that she'd had to pay money into a bank account to help fund the journey. Magashule was going to accept some award from an American institution, according to Els. When it turned out that he needed to pay for the accolade, he decided not to accept it. But the trip continued regardless. Els denied that the trip had been a way of showing her gratitude to Magashule for her company's RDP contracts.

In May 2012, the FSHS named Els 'Best Contractor of the Year for the role her company, Thutela Bogolo … played in helping the department meet its objective of building sustainable houses for the poor', according to *The Weekly*, which covered the occasion.[24]

The Govan Mbeki Awards, in which Els was honoured, were hosted

by human settlements MEC Olly Mlamleli, who was 'flanked' by Magashule, the newspaper reported. At the ceremony, Els described how she got ahead in the RDP business: 'I approached the [Mangaung metro] municipality and spoke with the mayor Thabo Manyoni and I offered to help the government build better RDP houses. He then linked me with the Free State premier, who subsequently gave me the opportunity to build one of the show houses that formed part of the government's building projects.'

'I would like to thank Mr Magashule for believing in me and for giving me a chance to showcase what I think every human being should have – a decent house,' she said in her acceptance speech.

I spoke to Manyoni who denied 'linking' Els with Magashule. 'She knew Ace and Hantsi [Matseke] long before me!' he protested.

Els's comments, no doubt unintentionally, confirmed the long-held suspicion that Magashule directly influenced the awarding of tenders in his provincial departments. Instead of obtaining contracts through a competitive bidding process or even through lobbying the department itself, Els seemed to be affirming that one had to win Magashule's approval to get a foot in the door.

Or maybe it simply came down to good-neighbourliness. As mentioned earlier, businessman Glen Netshivhodza was another Parys local and Magashule confidant who scored big during the housing department's R1-billion spending spree. Incidentally, Magashule's wife, Seipati, is in business with Netshivhodza's wife. Seipati and Elsie Netshivhodza are listed as co-directors of a company called Kumba Civils.

In March 2013, Netshivhodza was appointed chairperson of the Free State Tourism Authority, a troubled provincial government entity that

later merged with the provincial gambling board and liquor authority.[25] PH-138 Sources familiar with developments say that, as with nearly all major moves in his government, Magashule was behind Netshivhodza's appointment to the tourism authority.

Netshivhodza's two companies – Ithuteng Consultancy and Harakisha Building Construction – together pocketed more than R30 million from the FSHS, about R20 million of which was received during the first two financial years of Magashule's reign as premier.

Like some of the other connected contractors, Netshivhodza apparently failed to complete his houses. For instance, Harakisha was appointed in 2010 to build 400 houses in QwaQwa. By 2013, the company had not finished a single one of these units, according to a progress report. The FSHS was left with no choice but to terminate the contract. The project was then taken over by TTC, the company owned by soccer boss Mike Mokoena.[26]

This apparent inability to finish projects seems to be a common trait among the contractors from Magashule's circle.

The final contractors worth singling out are owned by businessmen Madoda Khoba and Tlale Mokgadi, both alleged to be close to Magashule.

Khoba is based in the former homeland of QwaQwa and is said to be one of Magashule's closest friends in this part of the province. His two companies, Group Two Trading Enterprise and Group YWO Trading Enterprise, earned an impressive R210 million in revenue from the FSHS between 2009 and early 2018, coinciding exactly with Magashule's rule as premier.

There is documentary proof that Khoba may have dished out bribes to clear certain regulatory obstacles. Records from a court case in the

North Gauteng High Court detail how he allegedly paid an official of the Construction Industry Development Board R6 000 to get a higher CIDB grading in 2007. A higher grading would have allowed Khoba's companies to bid for more lucrative government tenders, such as the ones he clinched in the Free State.[27]

Mokgadi's company, E'tsho Civils, is one of the private firms the FSHS appointed to draw up a report following the R1-billion debacle in 2010. But it has been doing well on the construction side of things too. Between 2011 and 2017, E'tsho Civils netted a cool R150 million in revenue from the department, the HSS shows.

A few of my sources told me that Mokgadi and Magashule 'travel the world together'. I found some evidence of this in the IgoFiles, the leaked documents I unpack in Part VII. A document from the premier's office shows that in early 2014 Mokgadi flew to Cuba with Magashule.

There is overwhelming evidence that a large slice of the pie in the Free State housing department's big splurge was gobbled up by contractors who either had tangible links to Magashule or were said to be close to him. In fact, R250 million was channelled to ten such companies in the two years between 2010 and 2012 alone. This included large payments to the likes of Blacky Seoe (a former business partner), Hantsi Matseke (a close friend from Parys) and Moreki Moroka (wife of a long-time lawyer pal).

But this was just the start of a process that would eventually see a mountain of money shift to people in Magashule's inner circle. These contractors, along with a few others who got in on the action only after the R1-billion splurge, altogether received a staggering R2 billion in revenue from the FSHS during the nine years of Magashule's reign as

premier.

His daughter, Thoko Malembe, started scoring FSHS contracts in November 2013. Unital Holdings, the company in which she is a 30 per cent shareholder, received contracts worth more than R150 million from the department for the failed Vogelfontein housing project outside Bethlehem. My work on this story for *News24* revealed that Magashule's office influenced the awarding of the contract, and that he visited the site in person after Unital was appointed.[28] Magashule denied influencing the awarding of the contract, but failed to or refused to comment on his daughter's stake in the company.

Despite clear indications that contractors linked to Magashule are among the worst culprits when it comes to failed, delayed or substandard RDP projects, these companies were excluded from the FSHS's attempts to recover wasted money.

In July 2015, the Democratic Alliance asked the department to provide figures on incomplete houses to the provincial legislature's portfolio committee on public works, infrastructure, roads, transport and human settlements. Mokhesi came back with a truly shocking number – there were almost 11 000 incomplete houses all over the province, the HOD admitted.[29] Another submission to the portfolio committee in 2018 failed to put a figure on the total number of incomplete houses, but it confirmed that the problem had not been resolved and that projects awarded to politically connected contractors during 2010 had still not been completed.[30]

The man who should be held accountable for this mess is Ace Magashule. As evidenced by the myriad examples unpacked in this chapter, Magashule clearly loomed large in the province's allocation of housing contracts during his time as premier. This allowed him to dish

out RDP contracts worth billions of rands to friends, family members, former business partners and other associates. Many of these contractors were completely unprepared for large RDP projects and consequently contributed to the scourge of unfinished houses that still affects poor people in the Free State today.

The fact that the auditor-general identified R7 billion in irregular expenditure at the FSHS during Magashule's time in office shows that there is much more to uncover. Furthermore, Open Water's handling of the 2010 contracts and the apparent derailing of the SIU investigation points to a massive cover-up that would have required the involvement of senior politicians.

So far, not a single top-level government leader has been held to account for one of the largest low-cost housing debacles in South African history.

COMMISSION OF INQUIRY INTO STATE CAPTURE

Guptas, Big Banks Linked to South African-Chinese Locomotive Deal

occrp.org/en/investigations/7257-guptas-big-banks-linked-to-south-african-chinese-locomotive-deal

Twitter

If you look closely at the details of a 2014 contract to bring Chinese-manufactured locomotives to South Africa, you can tell that something more than transportation was going on.

Photo: Bob Adams, flickr

On the surface, the contract referred to a big, seemingly conventional deal in which China South Rail, a state-owned Chinese manufacturer, would deliver locomotives to South Africa's state-owned transport infrastructure firm, Transnet.

China South Rail's contract for 359 locomotives was worth a whopping US$1.5 billion.

But this was no straight deal.

Behind the contract were associates of South Africa's wealthy and politically connected Gupta family, which has been implicated in an ambitious financial raid on Transnet, as previously reported by OCCRP. The Guptas have close ties to South African President Jacob Zuma, whose son, Duduzane Zuma, is on their payroll, and they are well known for giving perks to other public officials and receiving favors in return.

The contract shows China South Rail promising to pay $321 million as an advisory fee to Salim Essa, an alleged front man and proxy for the Gupta family.

For that fee -- which represented an astounding 21 percent of the total contract -- the Chinese identified Tequesta, Essa's Hong-Kong-registered advisory firm, as providing it with "Black Economic Empowerment" assistance. (All foreign investment in South Africa needs this designation, intended to correct the economic imbalances of the apartheid regime that ended in 1994.)

The fee was to be paid under an unusual arrangement spelled out in the contract that required Transnet to cover the cost. In short, the fee appears to be structured like a kickback to the Gupta empire that is funded by South African taxpayers.

Banking records obtained by the Organized Crime and Corruption Reporting Project (OCCRP) trace a total of $75 million paid out by China South Rail after the contract was signed and $39.8 million in the three months prior to that. OCCRP did not have access to all records to track the full $321 million in payments.

The documents show that the money went first to Gupta-associated companies and then on to a series of small shell companies where much it disappeared. But some is traceable to payments on everything from coffee to luxury cars. Bankers often failed to flag a suspicious scheme, accepting large payments from the Chinese rail firm and then paying out a series of smaller payments to an array of shell companies controlled by the Guptas.

After all this, South African taxpayers suffered the indignity that the first two locomotives that arrived in the country in early 2017 turned out to be defective. They never ran.

South African President Jacob Zuma (Photo: GovernmentZA, CC BY-ND 2.0)

Fixers

According to the contract, Tequesta, the Gupta-connected firm run by Essa, got an advance of ($60 million), which represented 3.9 percent of the contract before it was even signed. The rest was to be paid from money Transnet sent to China South Rail, which would then pay a portion of it on to Tequesta, or any other entity of Tequesta's choice.

As the contract put it, "Each time the company [China South Rail] receives a payment from the client [Transnet] as a percentage of the total contract value, same proportion of the advisory fee will be paid to Tequesta."

If Transnet stopped paying or reduced payments, the contract stipulated, Tequesta would get zero or reduced fees.

The banking data reveals that a total of $114.6 million was paid out by China South Rail in some 42 transactions. About $49 million was sent to Tequesta's HSBC account between June and October 2015. The remaining $65 million went into the HSBC account of a Hong Kong company called Regiments Asia, also throughout 2015.

In response to reporters' inquiries, HSCB representatives wrote that "HSBC simply has no desire to do any Gupta-related business. To the best of our knowledge, HSBC previously exited, is in the process of exiting, or never had a banking relationship with Tequesta, Regiments, ... [and persons such as] Mr. Salim Essa ... or other members of the Gupta family, and other Gupta-related entities we have become aware of through the media or otherwise."

Regiments Asia (of which Essa is a cofounder) and Tequesta are partners that share many of the same principals. The two firms were established on the same day, June 20, 2014, they share the same Hong Kong address.

According to whistleblower information provided to OCCRP, another alleged cofounder of Regiments Asia, Eric Wood, was at the time a shareholder in Regiments, Transnet's South African financial partner. (OCCRP recently reported a separate scheme in which Regiments and another firm overcharged Transnet for millions in unnecessary loan rate swaps.)

Via his communications company, Grit, Wood told OCCRP that he knew nothing about any of this. "Mr Wood ... unequivocally and categorically states that he has no knowledge of Regiments Asia" or any of the other companies mentioned.

A familiar pattern

Moving assets in this way, through confidential contracts and multiple shell companies, along with the use of well-placed allies in the government, is a Gupta specialty.

"Guptaleaks" is the name given to a recently published collection of Gupta business documents that came from a whistleblower. The emails and documents show Wood and the Guptas colluding with Transnet insiders to ensure that its rail supplier contracts went to companies of their choosing. China South Rail was one of those chosen.

Malusi Gigaba, then Minister of Public Enterprise, announces the appointment of Brian Molefe as Chief Executive of Transnet in 2011. (Photo: GovernmentZA, flickr) One of their insider allies was Iqbal Sharma, another Gupta associate and Essa's business partner, who was appointed to several senior Transnet positions. He was named to the company's board in late 2010 by then-Minister of Public Enterprise Malusi Gigaba, who has held a number of senior positions by appointment of President Zuma. By 2013 he had become chairman of Transnet's Board Acquisition and Disposal Committee alongside Anoj Singh, then the company's chief financial officer and since exposed as another Gupta associate, according to a report by South Africa's former Public Protector.

Singh was also key to the Guptas' efforts to influence Transnet. In fact, Transnet's tender for the locomotives came out in July 2012, the same month he was appointed.

In his crucial position, Sharma was in close contact with the Guptas and Wood as Transnet moved forward on the locomotive tender. As the Guptas' insider within the company, he was instrumental in steering the state firm's decisions in a way that made the scheme possible.

The Guptaleaks emails also show that Woods and the Guptas had access to a confidential internal Transnet document that spelled out the procurement criteria for the tender.

In the fall of 2014, media reports were beginning to point to the Guptas' influence on state entities, including Transnet. In response, the company hired

PricewaterhouseCoopers (PwC) to carry out an investigation.
That November, according to Guptaleaks documents, PwC had identified multiple Gupta-linked companies in which Sharma "might have" a conflict of interest because of his involvement in companies that benefited from deals with Transnet.

Sharma's own company, VRLS, also linked to Essa, was financially integrated into the Guptas' corporate empire, according to documents in OCCRP's possession. Meanwhile, Tequesta itself gave the company a multi-million-dollar loan, according to Tequesta's September 2014 balance sheet, also obtained from Guptaleaks.

Yet the Guptas' influence continued. The following year, in a memo obtained by OCCRP, Transnet retained Regiments to raise $800 million it needed to pay for the locomotives. (See: Guptas, Nedbank skillfully extract money from South African state firm)

Transnet ultimately wanted to buy a total of 1,064 locomotives; the Chinese-owned firm's ultimate allocation would soon increase from 359 to over 500.

Early in 2017, the first two of the locomotives were delivered and found to be unusable. While acknowledging "glitches," Transnet said that those two locomotives were simply prototypes. It is not known when delivery of the remaining locomotives is to take place.

Round and Round

China South Rail sent the locomotive deal "fee" to Regiments Asia and Tequesta in chunks ranging from $100,000 to several million dollars.

The bank data shows that, whenever Regiments Asia received a credit to its account, it was always from China South Rail -- suggesting that the firm had been established precisely for this deal. Tequesta records show a similar pattern, with 90 percent of its money coming from China South Rail.

But the money didn't stay with the two shell firms for long. The millions then went through more than three dozen shell companies around the world, mostly using HSBC accounts in Hong Kong and other locations, but also employing other banks in London, Johannesburg, Dubai, and the US.

Regiments Asia paid more than $100 million from its account to shell companies that appeared to have no substantive business activity, employees, or even physical offices. These companies, bearing names such as Gallenade, Success Stand, Shun Shi, Honorway, Bestway, PAI, Al Malaki, Vogen, Daya and Flybright, received money, sometimes almost daily, from late 2014 through February 2017, with the bulk arriving in 2015. Tequesta paid out over $60 million to the same shell companies.

Gupta family members received some of these funds directly in transactions flagged as problematic by big banks' compliance departments.

In all, OCCRP data shows that more than 20 banks sent or received money from

Regiments Asia, Tequesta, or the shell companies. Led by HSBC, these banks also included National Westminster in the United Kingdom, Wells Fargo in the US, India's state-owned Bank of Baroda, Habib Bank, Standard Chartered Bank, and a dozen Chinese banks like Bank of China and China Citibank. Often, the transfers were listed as "commissions."
Flows from one key conduit in South Africa, a shell company called Homix, were so vast that the account was shut down by its bank, Mercantile Bank, after just 11 days. During that time, the company -- which was allegedly run by Essa's legal advisor Ashok Narayan – sent $8.4 million to Morningstar International, a Gupta-controlled firm in Hong Kong.

Big banks like the Bank of Baroda and HSBC allowed the payments to carry on from 2014 until 2017. Mercantile, however, noticed suspicious activity within four working days of the account being opened. Its bankers reported this to the South African Reserve Bank, which requested that Mercantile block the account, which it did.

Like the other shell companies in the scheme, Homix appeared to have no substantive business activity or employees. But each remittance it sent to Morningstar had an instant consequence. For instance, on May 27, 2015, at precisely the time that Homix sent two payments to Morningstar International Trade, that company moved similar amounts to Gallenade and Billion Lucky. On the next day, the same pattern was repeated.

After Mercantile shut down the Homix account, and perhaps unknown to the bank, other nominees stepped in to serve as new conduits for Morningstar.

Some of the Morningstar funds ended up in the US with a company called MNT Trading, which received transfers from Morningstar's Hong Kong account in its account at Wells Fargo.

Between Tequesta and Regiments, more than $160 million was moved through international banks led by HSBC and Bank of Baroda.
A host of transactions by the Guptas, such as buying luxury cars, groceries, or even coffee and bagels at Pret-a-Manger in London, were also flagged as suspicious by the compliance departments of several big banks.

But the flagging appeared to make no difference, and the transfers continued.

South Africa's Parliamentary Portfolio Committee on Public Enterprises has investigated the influence of the Guptas on the country's state-owned entities, including Transnet. But there has been little scrutiny of institutions such as the Bank of Baroda, HSBC, and other banks that helped them, keeping transaction fees for themselves. In fact, transactions considered "risky" -- such as the large flows described here – brought the banks higher fees.

No Comment

China South Rail could not be reached at the time of publication.

Essa did not respond to reporters' questions.

Wells Fargo declined to comment, citing client confidentiality.

Habib Bank did not respond to questions concerning Essa's account.

Regiments categorically denied knowing anything about Regiments Asia and said its relationship with Transnet was "duly mandated," meaning legal.

Sharma told OCCRP that he "did not act improperly at any time during [his] time on the board of Transnet."

Transnet did not comment to questions about the validity of the locomotive contract, the role of Regiments, Regiments Asia, and Tequesta, or the commissions worth $114.6 million that OCCRP identified.

Time stamps show that all emails asking for explanations were opened and viewed.

This story is part of the Global Anti-Corruption Consortium, a partnership between OCCRP and Transparency International. For more information, click here.

It was supported by Trust Africa, a non-profit organizaton supporting investigative journalism and advocacy.

Twitter

PH-149

Guptas 'laundered' R52m in Hong Kong, #StateCaptureInquiry told

POLITICS / 8 JUNE 2019, 09:53AM / LOYISO SIDIMBA

Deputy Chief Justice Raymond Zondo, who chairs the Commission of Inquiry into State Capture. Picture: Karen Sandison/African News Agency (ANA)

Johannesburg - A SA Reserve Bank (Sarb) executive on Friday revealed shocking details of how a Gupta-linked company successfully moved almost R52 million from South Africa to Hong Kong and claimed it had bought goods worth about R50 000.

Shiwa Mazibuko, head of the Sarb financial surveillance department, told the Commission of Inquiry into State Capture that letterbox company Homix exported R51.8m through Mercantile Bank via an intermediary in 2015 before R14.4m was blocked.

Mazibuko said Homix was used to take money out of the country illegally and committed trade-based money laundering. "If this was not stopped, this could have been R500 million after some time," he said.

Commission chairperson Deputy Chief Justice Raymond Zondo asked why there was no system that prevented such large amounts of money from moving out of the country.

Mazibuko said it was difficult to trace each and every transaction as 500 000 foreign exchange transactions worth trillions of rand were processed daily.

RELATED ARTICLES

Graft at Transnet rampant under

#StateCaptureInquiry hears how former

Former A slams M

PH-150

Molefe, Singh, #StateCaptureInquiry told

Transnet official stopped R750m theft

Williams 'absolute

The Hong Kong beneficiaries were Morning Star International, to which 14 of the 16 transactions investigated were destined, and YKA International Trading Company, which received the remaining two.

Mazibuko said both companies had sole directors.

"It was a money laundering scheme," he said.

Homix was nominated by Gupta associate Salim Essa to receive payments from Transnet and Regiments Capital.

Essa initially nominated Chivita Trading to receive money from Regiments but later put forward letterbox company Homix.

Chivita was paid more than R80m in a few months in 2014 while Homix received about R95m from Regiments Capital.

Last week, the commission heard how Homix was paid R36m for facilitating a R1.8billion deal between Transnet and telecommunications network operator Neotel in December 2014 despite not adding any value.

Earlier this year, Standard Bank's former general counsel Ian Sinton said Homix received payments from Regiments on Essa's behalf.

According to Sinton, most of the funds transferred into Homix's Standard Bank account, which has since been closed, were from Neotel, Regiments, Cutting Edge Commerce, Digital Video Solutions and Sechaba Computing.

Most of the R324m transfers were later paid to Bapu Trading.

The commission also concluded the evidence of former Transnet treasurer Mathane Makgatho, who gave shocking testimony on how she feared for her life and being poisoned due to the toxic environment at the state-owned freight and rail transport company.

Makgatho said she was tipped off that there was a meeting in which Essa told the gathering she was a stumbling block, but never found out what it resolved.

She said she was completely paralysed when she was made aware that the Taiwanese Mafia was involved in the multibillion-rand deals that Transnet was negotiating with Chinese companies.

"It was rough. It was so bad that if I had opened a bottle of water and for some reason turned, I would not drink that water," Makgatho said, adding that she was afraid she would be poisoned.

"We were fighting so much that swear words became the order of the day," Makgatho recalled her 21-month tenure as Transnet treasurer.

Mazibuko will resume his evidence on Monday.

Political Bureau

Related Tags

Guptas

COMMISSION OF INQUIRY INTO STATE CAPTURE

How the Guptas Milked South Africa for Diamonds

occrp.org/en/investigations/8500-how-the-guptas-milked-south-africa-for-diamonds

Twitter

Under recently ousted President Zuma, the Gupta family made millions in South Africa. Some of that money may have been used to purchase diamonds in a scheme which defrauded a state program to help poor black dairy farmers.

Koos Mthimkhulu, a black cattle-farmer, inspects his herd at his farm in Eastern Free State Province, South Africa, 2012. Mthimkhulu was born on a white-owned farm, and at the end of minority rule in 1994 was selected for a reform program whereby the government bought agricultural land from white farmers and handed it over to blacks with legitimate claims on the territory. Photo: Reuters / Siphiwe Sibeko

Until a couple of years ago, Shrenuj Group was one of India's largest diamond and jewelry manufacturers. But to South Africans, Shrenuj may soon have a less glittering claim to fame — documents obtained by the Organized Crime and Corruption Reporting Project (OCCRP) show that the company was among those that received South African state funding stolen by the disgraced Gupta family.

In what was the country's first legal action against the Indian-born tycoons, their associates, and their group of companies, the high court heard from state prosecutors that case involved "proceeds of crime."

The prosecution argued that some 220 million rand (US$ 15.5 million) out of over half a billion rand in state funds allocated to the now infamous Estina dairy project had been stolen by the Guptas and their related entities. The farm, a project of the Free State provincial government, was intended to assist the province's poor black farmers.

But those vulnerable farmers are still waiting for what they were promised. A portion of the stolen money — 4.5 million rand ($317,800) — was transferred to Uxolo, a South African subsidiary of Shrenuj. The remainder was siphoned by the Guptas through suspicious transactions to other entities identified in a previous OCCRP report as being under their control.

That investigation, published by OCCRP and The Hindu on February 27, revealed how the Johannesburg branch of the Indian Bank of Baroda handled hundreds of millions of dollars in transactions tied to the Guptas. The brothers' allegedly corrupt dealings with former South African President Jacob Zuma and his family, specifically his son Duduzane Zuma, led to the president's resignation on February 14.

Duduzane has since been arrested on conspiracy to commit corruption and his passport seized. He was later released without charge, and then left the country.

In the case against the Guptas, South Africa's Asset Forfeiture Unit claimed that Shrenuj subsidiaries had received the Guptas' stolen millions at its Bank of Baroda account. Though Baroda transactions, reviewed separately by reporters, don't indicate their origin, they do confirm that two Shrenuj subsidiaries that held accounts at the bank had indeed received millions of dollars in deposits.

The case before the high court is now in limbo, with the judge ruling that prosecutors had not sufficiently proven their case, but that there was enough evidence of wrongdoing to keep the Guptas' assets restrained or "frozen." Meanwhile, a separate inquiry that is looking into the Guptas' so-called "state capture" of South Africa — including the funds at issue here — is proceeding.

The Guptas are still at large (they have since fled the country along with Duduzane Zuma). However, Shrenuj is no longer with us. In a move which its executives insist was entirely unconnected with the Gupta scandal, the company declared bankruptcy last year.

So how does one turn funds for a dairy farm into diamonds — and to what end?

Milking the Country Dry

The story began in the small farming town of Vrede in South Africa's Free State, a sprawling province of rolling hills and pastures that borders Lesotho. In 2013, the Free State government launched a project with a simple goal — to create a cooperative for

small-scale black farmers previously disempowered by apartheid. Locals interested in becoming "empowered" would sign up, receive training, and have the opportunity to join the cooperative.

All that was needed was capital from the provincial government — half a billion rand, according to initial estimates — and a private contractor to carry it out.

And while a handful of trainers arrived to help empower the locals, the vast majority of the promised funds never did. Instead, the contractor, a Gupta company called Estina Pty Ltd, walked away with the money while the fields lay fallow. According to the Asset Forfeiture Unit, just 2.4 million rand was actually invested in the project.

The case was politically significant as it represents the country's first legal action connected to the "state capture" scandal, which has rocked the country for months. Nevertheless, the Gupta brothers appear to have won round one, with the court ruling that 180 million rand ($14.4 million) of the 220 million the Guptas are accused of stealing may be unfrozen, according to media reports. OCCRP reporters, however, were told the assets were still under restraint.

That money seems to have been parceled out piecemeal to various front companies and persons within their business empire — some of it less obliquely, such as the ten million rand ($800,000) Atul Gupta, one of the three Gupta brothers, received directly.

Former South African president Jacob Zuma dines with Atul Gupta (right) during an SABC business briefing, Port Elizabeth, South Africa, March 2012. Credit: GovernmentZA / Flickr

Moving Millions

Transaction records from the Bank of Baroda obtained by reporters (and detailed in the earlier investigation) shed further light on some of the Guptas' transactions, covering a portion of the stolen funds under investigation by the court.

The records show that Estina held an account at the bank — and that 140 million rand ($13 million) was deposited into this account between July 2012 and August 2014. (Because of the form in which these records are structured, it is not possible to identify

the source of Estina's funds.)

Between October 2012 and January 2016, the records show over 126 million rand ($9.2 million) leaving the account.

Neither do the existing records indicate where the money was sent. But sums of identical value appeared in other Bank of Baroda accounts held or controlled by the Guptas, often within days.

Out of all the banking options present in South Africa, Estina's use of a Bank of Baroda account, a state-owned Indian bank, suggests the company's extremely close ties to the Guptas' business empire. The bank had long taken a lax approach to their illicit dealings, with its officials routinely voiding warnings of suspicious transactions raised by South African authorities. The Guptas dominated the bank to such an extent that the majority of its financial transactions were theirs.

In the high court case, prosecutors claimed that Estina — ostensibly founded to carry out the agricultural cooperative project envisioned by the state — had been a shell company all along, established by the Guptas to steal agricultural subsidies. Corporate records show that the company had no established track record as an agricultural enterprise.

Attempts to seek comment on the fate of the dairy money from the Guptas themselves and from Baroda's South African branch were unsuccessful. For its part, Shrenuj responded that the court order contained an "error in [its] assessment... Shrenuj Group, or its employees, have never been engaged in any transaction, business or otherwise, with the Gupta brothers or any of their entities. We categorically deny any affiliation or association with Estina or Gupta brothers. ... The money drawn was used to pay outstanding obligations within the diamond business operations of Uxolo [A Shrenuj subsidiary in South Africa which received the funds] and there was no third party beneficiary."

A commuter walks past an advertisement of Bank of Baroda in Kolkata, India, November 2015. The bank was once India's second-biggest state-run lender by assets. Credit: Rupak de Chowdhuri / Reuters

Diamonds Are a Gupta's Best Friend

If you're seeking to launder illicit funds, whether stolen from a dairy farm or anywhere else, diamonds are perfectly suited for financial skulduggery.

The trade in diamonds differs from the trade of any other mineral in that the value of the gems is determined subjectively by buyers and sellers, with very little oversight from external regulators.

As such, companies or individuals trading in diamonds can easily manipulate their values in different jurisdictions — a technique that can allow them to dodge taxes, shift profits abroad, or launder money.

So it's noteworthy that the transfer between Estina and the two Shrenuj subsidiaries is far from the only connection between the Guptas and diamonds. In The brothers have also tried to purchase a diamond mine in Lesotho.

HSBC bank records flagged as being related to the Guptas and seen by reporters show that the family also shifted money to a Hong Kong-based firm, Simoni Gems, that describes itself as a major supplier of fancy shaped diamonds on its website.

It is difficult to definitely establish what real business, if any, this company may be engaged in. Little information could be found about it beyond its website.

The firm, which held accounts at HSBC, shares a telephone number with Fancy Star, a Dubai-based company registered as a commodity trader. Dubai is not just the world's premier hub for laundering illicit diamonds; it is also a jurisdiction that, according to the Gupta leaks, played a major role in the brothers' laundering of billions of dollars from South Africa.

In April, South Africa's national prosecuting authority stated that it believes that millions of rand stolen by the Guptas from the Estina dairy farm indeed ended up in Dubai.

According to Indian corporate data, Simoni Gems is also registered in the country under a different name — Shivani Gems — which, though listed as a furniture manufacturer (and originally launched as a media company), presents itself as a diamond trader.

Shivani has an outlet in the United States — a country to which the Guptas appeared to regularly funnel money via other companies with HSBC accounts. The directors of Shivani Gems include several people with the Gupta surname which corporate data shows had been marked as "politically exposed persons." Atul Gupta's wife is named Shivani.

"If the Guptas criminal network exploited the diamond trade for money laundering purposes, they wouldn't be the first," says Hennie van Vuuren, an anti-corruption activist and director of Open Secrets, a South African NGO. "Investigative journalists and government agencies have shown how diamond-trading behemoths like De Beers have historically undervalued diamonds and thereby effectively defrauded tax authorities and the treasury. What we see here may well be more of the same."

With South Africa still reeling from the scale of the Gupta scandal, the ultimate fate of Estina's dairy money deepens concerns about the role of the Bank of Baroda in facilitating the brothers' mass embezzlement of state assets.

If these stolen funds have indeed been converted into diamonds, they'll be a headache for authorities to trace, and a nightmare to return to the state's coffers to be spent as originally intended.

A sweet opportunity for the Guptas became another sour promise for the country's poor black fairy farmers — still poor, and still waiting.

This story is part of the Global Anti-Corruption Consortium, a partnership between OCCRP and Transparency International. For more information, click here.

Clarification (August 25, 2018): This story has been updated to more clearly convey the fact that Simoni Gems is not a Gupta entity.

Twitter

LIKE THIS STORY?
HELP US HIRE REPORTERS TO DO MORE.
Donate here

The house of Gupta

amaBhungane | Scorpio

L35, the R325-million Dubai mansion, has emerged as one of the greater mysteries of the #GuptaLeaks.

On the one hand, L35 may offer proof that the Guptas have externalised vast amounts of money, stashing it conveniently in Dubai property. On the other, it has been alleged to be the smoking gun - the bribe the Guptas paid to President Jacob Zuma in the form a lavish 10-bedroom retirement home.

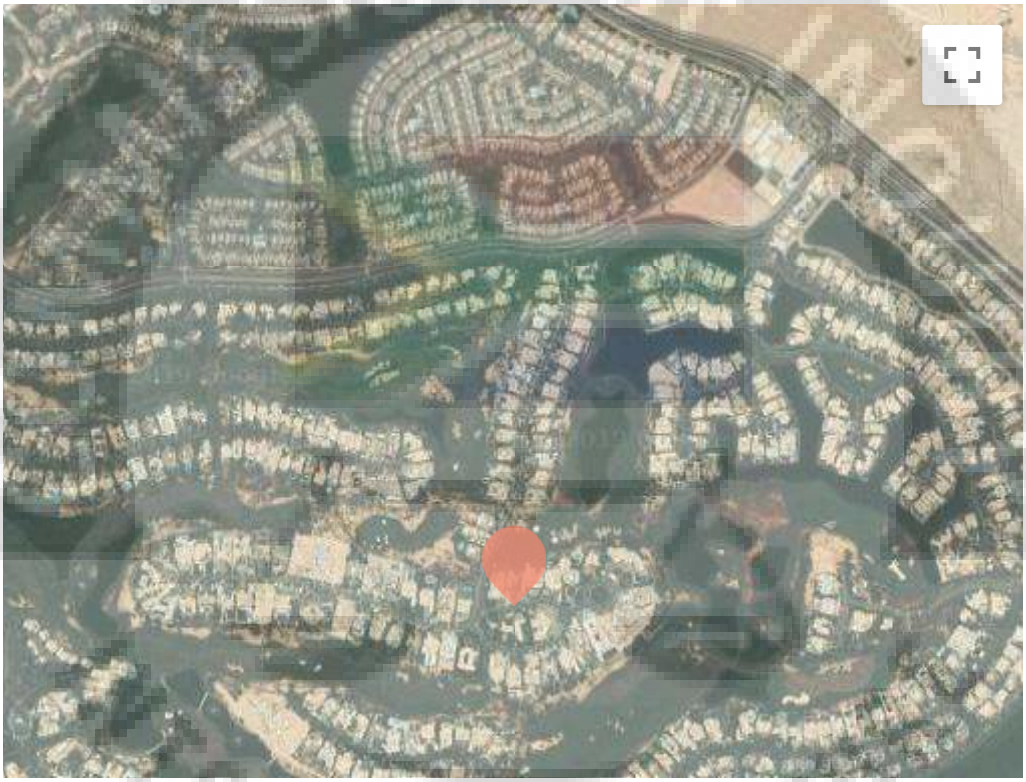
The verdict is still out... but here is what we know so far.

Inside L35: When estate agents Knight Frank put L35 on the market for AED 110-million (R384.6-million) in March 2015, their promotional material included this 3-minute video, giving potential buyers a glimpse at a villa they describe as "awaiting a VVIP ... with deep pockets." (Source: YouTube)

The Guptas go shopping

In April 2015, the Guptas started shopping for a property in Dubai.

Six properties were on the list for Tony Gupta's first day of viewings. At $30.5-million (R391.7-million), L35 was by no means the most expensive property - a "palace" on the tip of the Palm Jumeirah's VIP frond was on the market for $68.2-million (R875.9-million). But it was L35 that caught the Guptas' eye.



Dubai's most exclusive postcode: L35 sits on the corner on Lailak 2 street and Lailak 3 street, identifiable by the two squares on the roof (just to the left of the red marker). The gated suburb of Emirates Hills is known as "Dubai's most exclusive postcode" with views of the city and the Montgomerie golf course.

Pictures from the estate agents' website shows a 10-bedroom, 13-bathroom villa of white marble and gold trimmings, with parking space for 11 cars.

The asking price was AED110-million (R384.6-million) but the Guptas finally beat down the seller, Lebanese businessman Adib Hassan Ataya, to AED93-million (R325.1-million).

Here's where the picture gets a little murkier...

The secret owner

At this early stage in exploring the #GuptaLeaks it is not clear who the final buyer was for L35.

Documents clearly show Tony Gupta, the youngest of the three Gupta brothers, was listed as the original buyer. However, draft agreements show that as negotiations progressed, two off-shore companies - first Radiant Green and then Mahila Investments - were slotted in as potential buyers.

NOVATION AGREEMENT

(The "Agreement")

Entered into this day the __th of July, 2015 by and between:

1. ADIB HASSAN ATAYA of P.O Box 2639 Dubai, UAE (The "Seller");
2. RAJESH KUMAR GUPTA holder of Passport No [redacted] Republic of South Africa (The "Original Buyer");
3. MAHILA INVESTMENTS LTD., an Offshore Company registered at Jebel Ali Free Zone, PO Box 27430, Dubai, UAE (The "New Buyer").

Offshore, off limits: A draft agreement to register L35 in the name of Mahila Investments, an offshore company whose owners are never revealed. (Source: #GuptaLeaks)

Both Radiant Green and Mahila are registered in the Jebel Ali Free Zone where offshore secrecy laws mean the beneficial owners of the companies are never revealed.

Zuma's retirement plan?

When *Sunday Times* journalists visited Dubai last year, several sources reportedly told them that the Guptas had bought Zuma a multi-million-rand retirement home in Emirates Hills. L35 certainly fits the bill.

Further evidence that L35 may be President Zuma's "plan B" is contained in a letter drafted ostensibly for Zuma by Gupta lieutenant Ashok Narayan in January 2016.

The letter, addressed to the emir of Dubai, includes the line:

"I am happy to inform you that my family has decided to make the UAE, and specifically Dubai, a second home and have already acquired a residence located at Emirates Hills, Dubai (Villa No. L-35, Lailak Street No.1). It will be a great honor for me and my family to gain your patronage during our proposed residency in the UAE..."

But given the Guptas' apparent propensity for name-dropping and the fact that this is a draft, this letter is not conclusive.

I fondly remember our meeting in the UAE and the gracious hospitality and warmth extended to me during my visit. It is with this sentiment that I am happy to inform you that my family has decided to make the UAE, and specifically Dubai, a second home and have already acquired a residence located at Emirates Hills, Dubai (Villa No. L-35, Uplink Street No.1). It will be a great honor for me and my family to gain your patronage during our proposed residency in the UAE especially around security issues since my son and the family will be travelling quite extensively in and out of the UAE.

To this end I would be grateful if would kindly grant an audience to my son, Mr. Duduzane Zuma to meet with you and formally introduce the family to you.

I look forward to your guidance and direction in the above matter and remain with the best wishes,

Yours sincerely,

Jacob G. Zuma
President of South Africa

Zuma's second home: The letter drafted by Gupta lieutenant Ashok Narayan for Jacob Zuma. It's not clear if Zuma received the draft - similar drafts that do not mention L35 were sent to his son, Duduzane.

Zuma's spokesperson has denied that the president owns L35, and the ANC Women's League has called on *Sunday Times* to produce the title deeds of L35 showing that Zuma's name is on it.

PresidencyZA
@PresidencyZA

The story in the Sunday Times newspaper today, that President Jacob Zuma owns a "palace" in Dubai is a fabrication. bit.ly/2sDfsF8

245 9:17 AM - Jun 4, 2017

984 people are talking about this

However, if L35 is Zuma's mansion, it's unlikely to be registered in his name, but instead in one of the many black-box companies that make up the Guptas' UAE empire. And unlike South Africa where property records are publicly available, Dubai does not allow access to property records to anyone except the owner of the property.

Or a Gupta palace?

However, there's also evidence to suggest that L35 is merely the Guptas' "plan B", the foreign bolt-hole that they fled to when pressure started to mount in early 2016.

For one, the #GuptaLeaks show that the family commissioned extensive renovations and refurbishments of the Middle-Eastern themed mansion, including installing Persian carpets, a massive free-standing safe, and what appears to be the family's crest – in-laid in gold on interior doors.

Photos taken of L35 in April last year show the same Gupta family crests were bolted to the exterior gates after the property was bought.

The crest features the face of a lion or tiger, the city of Saharanpur, and the words "1892", "Lala Dhramdas Gupta" and the website address "Singhala.com" - an internet search shows the website was registered by the Guptas' Sahara Computers.

Family pride: The Gupta family crest mounted on the wall outside L35. This photo was taken in April 2016 after L35 had been bought by the Guptas.

The family palace: 3D renderings of proposed alterations to L35 show what appears to be the Gupta family crest emblazoned on interior wooden doors. (Source: #GuptaLeaks)

Another Dubai property

However, L35 was not the only property the Guptas were interested in. The #GuptaLeaks shows that they played a central role in helping Duduzane Zuma to acquire a AED5-million (R17.5-million) apartment in the Burj Khalifa tower.

It also shows that in March 2016, the Guptas were shopping for another house and were sent details about an 8-bedroom mansion for AED185-million (R646.7-million) just down the road from L35 that the estate agent points out "may be of interest for other family members".

At this stage there is no confirmation that the Guptas bought this property. For now the investigation continues.

Inside L35: More of the glamorous promotional photos of L35. (Source: Knight Frank.)

NEWS 09/04/2018 13:50 BST | **Updated** 09/04/2018 15:41 BST

Following Guptas' Temple Money-Laundering Trail

A temple under construction in their home town of Saharanpur was allegedly used in Gupta money-laundering schemes.

Jean le Roux
News 24

GALLO IMAGES VIA GETTY IMAGES

Ajay Gupta and younger brother Atul Gupta. Johannesburg, March 2, 2011.

A R200-million temple, built in honour of the Gupta brothers' late father, Shiv, was erected in their home town of Saharanpur using money laundered through several of the Gupta brothers' Indian and Dubai companies.

In

pr

Th

SUBSCRIBE TO THE NEWS NEWSLETTER

address@email.com

Subscribe!

SP

PH-166

Despite the Guptas themselves footing the bill for the construction of the temple, a local Indian politician, Mansoor Badar, and Sanjay Grover, a known Gupta lieutenant in Dubai, were used as the "donors" of the money earmarked for the temple's construction.

Contact Us Standards And Corrections User Agreement Privacy Policy Comment Policy Supply Chain Transparen X

In this multi-part investigation, we consider how the Gupta family laundered money using companies set up in Dubai and India, freeing them up to fund the temple's construction.

First stop: Saharanpur

Construction started on the Shiva Dham temple, located in the northern outskirts of the Gupta brothers' hometown of Saharanpur, in June 2014. The temple complex consists of several buildings, including the main temple itself, and a hall designed by architectural firm Trivedi Corporation in India.

The temple was still under construction in January this year.

And while documents in the Gupta leaks claim that Badar and Grover are the sole funders of the temple's construction, at least a portion of the donations was bankrolled by the Guptas themselves, making fools of Indian revenue authorities in the process.

To get the money into India, the Guptas needed a plan. The Gupta leaks show that Tony Gupta expressed an interest in establishing the family's own religious trust early in 2014.

Th

au

"W

es

ter

SUBSCRIBE TO THE NEWS NEWSLETTER
address@email.com
Subscribe!

Muhammad Saloojee, director and head of corporate tax at KPMG, on June 30, 2014.

PH-167

READ: Guptas dodge another tax deadline

Between June 2014 and December 2014, the family appeared to have abandoned

Contact Us Standards And Corrections User Agreement Privacy Policy Comment Policy Supply Chain Transparen X

Gupta leaks show that the temple's construction was overseen and paid for by an entity called Sh Siv Mandir Gor Sankar Vishwana Banunth Dham and Samsa Bumi Prabndak Saba (the Siv Mandir trust), a religious trust founded in 1990. The Siv Mandir trust was responsible for paying service providers and labourers for the construction of the temple.

The reasoning behind using a trust was economic: in terms of Indian tax laws, a religious trust can apply for favourable treatment of its own income as well as any donations made by its funders.

On December 10, 2014, Atul and Tony Gupta drafted a letter on behalf of their mother, the Gupta matriarch Angoori Gupta. The letter begged the Indian revenue authorities to grant the Siv Mandir trust exemptions from certain tax regimes.

Atul Gupta and his mother Angoori at the laying of the temple foundation stone. (www.shivadham.in)

"This temple is being constructed at the total project cost of [about R180-million]; the donation for which will be contributed by all individual persons in Saharanpur – and [a] major portion of this donation will come from Smt Angoori Devi Gupta and her family members and friends from all over the world.

"Trust has also applied for Income Tax Exemptions u/s 12 A of [Income] Tax Act and will also apply for exemption u/s 80 G of Income Tax Act. Once these exemptions are granted by the appropriate authority's [sic] donation [sic] from all across the world will start flowing in."

The letter was addressed to the tourism minister in Uttar Pradesh, the province of the Guptas' hometown of Saharanpur, appealing to the minister to intervene with the tax authorities.

Th
usi

Wi
be

SUBSCRIBE TO THE NEWS NEWSLETTER
address@email.com
Subscribe!

PH-168

Funnelling the funds

The Gupta leaks show that the temple had two intended sources of income. The first

Contact Us Standards And Corrections User Agreement Privacy Policy Comment Policy Supply Chain Transparen X

25-million rupees [R4.5-million] towards the construction of the temple.

As part of the donation, Badar was required to submit a letter containing very specific wording to the revenue authorities. The accountant for the family's businesses in India, Ashok Khandelwal, drafted an example of the letter to be used.

Khandelwal initially denied any role in the funding of the temple construction.

"Without going into the merits of your allegations, we have absolutely nothing to do with the so-called temple construction with which you are trying to associate our name," he wrote in an email.

"We would have no problems if you were publishing the truth, but publishing false stories without any facts should not be done. If you have any evidence, of our involvement in this, kindly share the details of the same with us before publishing the story in order for us to respond, because your inference of the information, if any, that you have seems to be absolutely wrong."

READ: Gupta fight goes to Dubai

Khandelwal failed to respond when confronted with a copy of the donation letter he drafted. He also failed to clarify why he drafted the letter under instructions from Gupta family associates if the donor was Badar, an apparently unrelated party. Instead, Khandelwal threatened legal action on the basis of defamation and blackmail in response to the questions posed.

Badar's motivation appears to have been political. In December 2014, Gupta lieutenant Ashu Chawla received two letters introducing Badar to the leader of a local political organisation. The letters, which had to be translated, introduce Badar to the leader of the Samajwadi Party, Akhilesh Yadav, and propose Badar as an ideal candidate for the ele

Bo
20
res

SUBSCRIBE TO THE NEWS NEWSLETTER
address@email.com
Subscribe!

But Badar was not about to use his own money to fund the temple, and this is where the laundromat kicked in. The Gupta leaks indicate how it worked.

Contact Us Standards And Corrections User Agreement Privacy Policy Comment Policy Supply Chain Transparen X

(Graphic: Jean le Roux and Jaco Grobbelaar)

Using several back-to-back payments, the true source of the funding would be hidden behind several layers of transactions. All of these companies are either under the direct control of Gupta family members, or their close associates.

The next day the cycle is repeated. ITJ Retails pays LCR Investments, who in turn pays Anil Gupta. Anil Gupta arranges for the funds to be transferred by unknown means to Badar, who in turn pays ITJ Retails.

This cycle was repeated for several days until about 21-million rupees [~R3.9-million] was paid to ITJ Retails by Badar.

But the trick lies herein: Badar never paid ITJ Retails. By skipping the last link in the chain, Badar would in effect "borrow" the money from ITJ Retails by not paying it over. This was confirmed by the balance sheet for ITJ Retails, which showed that as at March 4, 2014, Badar was owed exactly 23-million rupees [~R4.3-million] – the same amount contained in the planned budget for the temple.

The modus operandi becomes even clearer in another string of transactions or journal entries ordered a year later.

SUBSCRIBE TO THE NEWS NEWSLETTER
address@email.com
Subscribe!

Contact Us Standards And Corrections User Agreement Privacy Policy Comment Policy Supply Chain Transparen X

On March 6, 2015, another Gupta lieutenant Suresh Tuteja again requested that several pa
aff
Kh
pre

SUBSCRIBE TO THE NEWS NEWSLETTER
address@email.com
Subscribe!

Th
23-million rupees he lent ITJ Retails. Badar would then make a 23-million-rupee payment

PH-171

to the "temple".

Akash Khandelwal denied that he received or made any such payments, but would not

the money to be paid to ITJ Retails.

The entries also showed that the "temple" would in turn be used to settle a vehicle loan for the benefit of SES Technologies, another Gupta-linked company that will feature prominently in the next instalment.

We can now trace a trail from the temple trust to Badar and eventually LCR Investments and SES Technologies.

Going global

The source of the money received from LCR Investments and SES is a bit murkier. But the Gupta leaks show how these companies were used to launder money paid from several overseas sources.

The first of these sources were donations paid by the Gupta family from South Africa. In late 2013, Rajesh Gupta, his wife Aarti, and Atul's wife, Shivani, each gifted R1-million to their sister in India, Achlia.

Achlia Gupta is the sister of brothers Ajay, Atul and Rajesh, and is married to the same Anil Gupta mentioned above who provided Badar with the money to pay ITJ Retails. The donations made in late 2014 appear to have been made directly into Achlia's account.

The donations made to Achlia would invariably find their way back into the LCR Investments' and SES Technologies' laundry cycle. Bank records for SES show that Achlia frequently made large deposits into its account, which were subsequently funnelled away. Achlia and other members of the Gupta family, frequently made large unsecured loans to Gupta-linked companies, among them LCR Investments.

Payments made to LCR Investments by Gupta-owned companies in Dubai were a second so

to

Inv

An

pre

SUBSCRIBE TO THE NEWS NEWSLETTER
address@email.com
Subscribe!

PH-172

In response, Achlia referred to a donation made to her by Shivani "out of her natural love and affection for me and the same has been accepted by me".

money was paid from her sister's Bank of Baroda account into that of the Dubai-based Global Corporation LLC. Global Corporation would in turn pay this into the bank account of LCR Investments, again funding the cycle.

ALSO READ: Dubai: the Guptas' city of shells

Global Corporation was one several Gupta-linked shelf companies that a News24 investigation last year was unable to track down, despite journalists spending a week in Dubai.

A third source of funds was direct payments from the Guptas' Dubai-based companies. An elaborate example of the way the money is laundered is found in the Gupta leaks, and involves several companies that the Guptas have direct control over.

This laundering process will be delved into in the next instalment, as well as its links to the family's Dubai operations.

Since submitting our enquiries to the affected parties, the temple's website has been taken down. Archived versions of the website can be found here and here.

- News24

BEFORE YOU GO

SUBSCRIBE TO THE NEWS NEWSLETTER

address@email.com

Subscribe!

Jean le Roux
News 24

Suggest a correction

Contact Us Standards And Corrections User Agreement Privacy Policy Comment Policy Supply Chain Transparen X

GuptaLeaks Guptas News state capture translated South Africa

Conversations

0 Comments Sort by **Oldest**

Add a comment...

Facebook Comments plugin

Sponsored

12 Stylish Puffer Jackets That Will Actually Keep You Warm

Fall 2019 Boots To Covet From Ankle Booties To Knee-Highs

Become a US citizen. Find out if you can apply

U.S. Green Card - Free check

Sponsored Links

You May Like

Born Between 1955 and 2001? You Might Be Eligible For This New Life Insurance

Stangen

Learn How an Investment of R3000 May Lead to Long Term Profits

Vici Marketing

ed Links

SUBSCRIBE TO THE NEWS NEWSLETTER

address@email.com

Subscribe!

ed Links

Recommended For You

PH-174

This Is What A Hymen Actually Does And Doesn't Do

South Africans In Port Elizabeth Are Snapping Up This New Life Insurance
Clear Plan Life Insurance Quotes
Sponsored Links

COMMISSION OF INQUIRY INTO STATE CAPTURE

SUBSCRIBE TO THE NEWS NEWSLETTER
address@email.com
Subscribe!

PH-175

Gupta wedding: These are the most insane expenses for next week's R427m ceremony

If you marry into the family, one thing's guaranteed: A good party. This latest Gupta wedding takes place next week, and the bill is already astronomical.

by Tom Head — 2019-06-12 11:45 in Lifestyle

Ajay Gupta at the launch of ANN7 news channel on August 21, 2013, in Johannesburg, South Africa - Photo by Gallo Images / Sunday Times / James Oatway

2.4K
SHARES

There really is no wedding quite like a Gupta wedding. The Indian billionaires know a thing or two about b
cash, especially when it's been supplied by the South African taxpayer.

However, the family are hosting the mother of all ceremonies next week as the sons of Atul and Ajay Gup

We are conducting a quick survey to help us better understand what our site visitors like and to learn a little bit more about you

The week-long ceremony will be an exercise in ostentatiousness, blowing the Sun City wedding of Vega Gupta out of the water. Valued at R427 million by the Indian media, this upcoming double wedding will cost 14 times more than the South African ceremony which unleashed a political backlash.

But where is all that money going, and how will it be spent? Here's what we've managed to establish…

Also **Read**

- **Africa Unite: Local artists boycott Burna Boy inclusion in concert lineup**
- **Watch: Uzalo latest episode, Tuesday, 12 November 2019**
- **Watch: Generations The Legacy latest episode – Tuesday, 12 November 2019**
- **Watch: Latest Skeem Saam episode for Tuesday, 12 November 2019**

Gupta wedding in India – what luxuries will there be?

The location itself is going to cost the brothers a fair whack: They have rented out an entire luxury ski resort, high up in India's Himalayan mountain range. Auli is going to host hundreds of extended Gupta family members and close friends, from its vantage point of 10 000 feet – about three kilometres above sea level.

The sky-high venue won't be easy to reach, but the Gupta brothers have already got it sorted. They've splashed out millions to ferry their guests from lower ground to the heights of Auli. About 200 choppers will be used in total, as guests begin to arrive before the weekend.

Meanwhile, the guest list itself is going to be pretty swanky – a range of Bollywood stars and highly-connected politicians are expected to make the trek up the mountains. However, we don't expect to see Jacob Zuma making his way there – it seems to be a strictly local affair.

Of course, with all these movers and shakers – and the inevitably-awkward eating habits of certain family members – this party has to be extremely well catered. According to eNCA, the billionaires are once again one step ahead of the game – around 400 different options are expected to feature on the food menus. Now THAT'S out kind of wedding!

A few lavish extras

The lavish spending doesn't stop there, either. Ahead of this unfathomably expensive Gupta wedding, invites were distributed via silver boxes, weighing almost five kilograms each. The proud fathers are importing fine flowers from Switzerland, which also come with a bill for "tens of thousands" of plant pots.

Despite being chased out of South Africa by a tidal wave of public anger and judicial fury, the architects of state capture seem to be getting by just fine without plundering our state resources. If they ever feel like returning R427 million of their loot to Mzansi, we'll be waiting right here.

Tags: India The Gupta Family Weddings

PROTECTED DMCA

These Twins Were Named The Most Beautiful In The World, Wait Until You See Them Today
IcePop | Sponsored

13-Yr-Old Builds Own House For $1,500: Look When He Opens Door And Reveals 89 Sq Ft Masterpiece
DirectExpose | Sponsored

When is the Green Card Lottery 2021 deadline? Apply Now!
U.S. Green Card - Free check | Sponsored

Remember Pauley Perrette? Try Not To Smile When You See Her Now
PsychicMonday | Sponsored

Learn How an Investment of R3000 May Lead to Long Term Profits
Vici Marketing | Sponsored

We are conducting a quick survey to help us better understand what our site visitors like and to learn a little bit more about you

Anti-Snoring Device Everybody in South Africa Is Talking About
SilentSnore | Sponsored

Oprah's Mansion Costs $50M, And This Is What It Looks Like
LoanPride | Sponsored

THIS is the man Meghan Markle was married to before she met prince Harry!
Tips and Tricks | Sponsored

South Africa: New Wifi Booster Stops Expensive Internet
Money News Tips | Sponsored

Where Celine Dion Is Living At 51 Is Not Normal And Here's Why
Finance101 | Sponsored

15 Most Dangerous Bridges In The World
www.travelden.co.uk | Sponsored

15 Foods That Are Killing You Slowly
Kingdom of Men | Sponsored

A Look Inside Trevor Noah's New $20M Luxury Home in Los Angeles
Mortgage After Life | Sponsored

23 Hot Christmas Gifts That May Sell Out This November
Tech Discount Zone | Sponsored

Man Buys New House. Then His Gut Tells Him To Dig In His Backyard
The Travel Breeze | Sponsored

Is This the Solution To South Africa's Mosquitos We've All Been Looking For?
Moskinator | Sponsored

They Took The Same Photo For 40 Years. Don't Cry When You See The Last!
Meanwhile | Sponsored

Do You Drink Cola? Use it For the Following 12 Chores
Storiosa | Sponsored

Top 30 Most Beautiful Women in the World
Healthysoulmag | Sponsored

Revealed: Here's what professional rugby players earn in SA each year
TheSouthAfrican

Watch: Siya Kolisi shows off World Cup trophy to Miss SA [video]
TheSouthAfrican

We are conducting a quick survey to help us better understand what our site visitors like and to learn a little bit more about you

SUBSCRIBE to our Newsletter

Your email address

SUBSCRIBE

Terms and Conditions

We are conducting a quick survey to help us better understand what our site visitors like and to learn a little bit more about you

NEWS

Jesse Hess: Cousin becomes main suspect, on the run after alleged rape

BY ANDREA CHOTHIA 2019-11-13 12:06

The cousin of murdered Jesse Hess is said to be the main suspect after raping a 16-year-old girl in Hanover...

READ MORE

Durban traffic: Fatal M7 tanker crash causes huge fireball [video]

2019-11-13 11:45

Khama Billiat credits defence for Kaizer Chiefs resurgence

2019-11-13 11:21

TheSouthAfrican.com is all about South Africa and the stories that affect South Africans, wherever they are in the world.

We're independent.
No agenda.
No Bias.

Follow Us

Our offices are for administrative purposes only, no visitors will be accepted without an appointment.

South Africa– Blue Sky Publications (Pty) Ltd – Company Registration Number: 2005/028472/07.
Address: V&A Waterfront, Cape Town, 8001.

United Kingdom– Blue Sky Publications Ltd – Company Registration Number: 04683692.
Address: Riverbank House, 1 Putney Bridge Approach, London, SW6 4TJ

We are conducting a quick survey to help us better understand what our site visitors like and to learn a little bit more about you

PH-180

south africa

Copyright © Blue Sky Publications Ltd. All Rights Reserved.
thesouthafrican.com is a division of Blue Sky Publications Ltd. Reproduction without permission prohibited. PROTECTED DMCA

COMMISSION OF INQUIRY INTO STATE CAPTURE

We are conducting a quick survey to help us better understand what our site visitors like and to learn a little bit more about you

PH-181

The Guardian

This article is more than **5 months old**

Spend £2.7bn more to tackle organised crime, says NCA chief

Lynne Owens to make challenge to ministers during launch of strategic assessment

Vikram Dodd *Police and crime correspondent*

Tue 14 May 2019 00.01 BST

The government needs to find an extra £2.7bn to tackle the growth in serious and organised crime that is causing "staggering" damage to the United Kingdom, according to the director general of the National Crime Agency.

Lynne Owens is due to make the direct challenge to ministers on Tuesday as she launches the agency's annual national strategic assessment mapping out dangers from cyber crime, child sexual exploitation, drugs and other serious and organised crime.

The NCA, which was set up by the Conservative government in 2013, says there are at least 181,000 people linked to serious and organised crime in the UK - twice the size of the British army.

There are 37,000 active organised criminals and 144,000 people in the UK "registered on the most harmful child sex abuse ... dark web sites," the agency says, insisting its estimates are conservative and not scare tactics.

PH-182

Owens is due to tell the launch event in central London: "Serious and organised crime in the UK is chronic and corrosive; its scale is truly staggering. It kills more people every year than terrorism, war and natural disasters combined. Serious and organised crime affects more UK citizens, more frequently than any other national security threat.

The agency estimates serious and organised crime costs the UK £37bn a year, equivalent to £2,000 for each family.

Owens is calling for an extra £650m to be given to the NCA and for £2.1bn to fund agencies such as the Border Force and go to police efforts fighting serious and organised crime.

She will say: "We need significant further investment to keep pace with the growing scale and complexity. Some will say we cannot afford to provide more investment, but I say we cannot afford not to."

The sum asked for is the equivalent to a half penny on income tax, but comes as other demands are being made to provide extra funding for the police and other key public services.

A full spending review is supposed to happen within months but there is increasing expectation the tumult caused by Brexit may mean it is postponed until after the UK has made a decision on its future in the EU.

Owens will say: "The choice is stark. Failing to invest will result in the gradual erosion of our capabilities and our ability to protect the public."

The assessment warns that Brexit could "impact the prevalence of bribery and corruption over the next five years, as UK companies potentially come into greater contact with corrupt markets".

Referrals for key crime types are increasing, with some of the rise accounted for by better reporting and increased awareness. Modern slavery referrals are up 80% since 2016, and about 2,000 county lines drug routes are in use compared with 720 a year earlier.

The NCA says some organised crime groups are made up purely of children and young people "adopting businesslike operating models rather than relying on identity or postcode".

The agency warns of corruption among public officials, especially at the border, and among professionals such as solicitors and accountants who do the bidding of those involved in serious and organised crime.

A Home Office spokesperson did not directly address the call for more money, but said: "We continue to invest in the right capabilities and tools in law enforcement, across government and in partnership with the private sector."

John Apter, who chairs the Police Federation, said government cuts to policing, of around 19%, had helped serious and organised crime flourish. "This is the reality of years of austerity where we have seen the number of police officers reduced by almost 22,000 as the number of organised criminals has increased; the NCA is therefore right to say considerable investment is needed," he said.

Diane Abbott, the shadow home secretary, accused the government of being in denial, adding: "If the Tories were genuine about tackling serious and organised crime, they would provide all the funding that's needed."

More people in South Africa...

PH-183

... like you, are reading and supporting the Guardian's independent, investigative journalism than ever before. And unlike many news organisations, we made the choice to keep our reporting open for all, regardless of where they live or what they can afford to pay.

The Guardian will engage with the most critical issues of our time - from the escalating climate catastrophe to widespread inequality to the influence of big tech on our lives. At a time when factual information is a necessity, we believe that each of us, around the world, deserves access to accurate reporting with integrity at its heart.

Our editorial independence means we set our own agenda and voice our own opinions. Guardian journalism is free from commercial and political bias and not influenced by billionaire owners or shareholders. This means we can give a voice to those less heard, explore where others turn away, and rigorously challenge those in power.

We hope you will consider supporting us today. We need your support to keep delivering quality journalism that's open and independent. Every reader contribution, however big or small, is so valuable. **Support The Guardian from as little as $1 - and it only takes a minute. Thank you.**

Support The Guardian

PH-184

Topics

- NCA (National Crime Agency)
- Police
- Crime
- Organised crime
- news

COMMISSION OF INQUIRY INTO STATE CAPTURE

COMMISSION OF INQUIRY
INTO STATE CAPTURE

News

October 2019

September 2019

July 2019

June 2019

May 2019

April 2019

March 2019

February 2019

January 2019

2018

2017

2016

2015

2014

2013

2012

Case Updates

News Releases

Speeches

Statements

For news, speeches or statements published before April 2012, please see our archived sites.

SFO agrees first UK DPA with Standard Bank

30 November, 2015 | News Releases

The Serious Fraud Office's first application for a Deferred Prosecution Agreement was today approved by Lord Justice Leveson at Southwark Crown Court, sitting at the Royal Courts of Justice.

The counterparty to the DPA, Standard Bank Plc (now known as ICBC Standard Bank Plc) ("Standard Bank"), was the subject of an indictment alleging failure to prevent bribery contrary to section 7 of the Bribery Act 2010. This indictment, pursuant to DPA proceedings, was immediately suspended. This was also the first use of section 7 of the Bribery Act 2010 by any prosecutor.

As a result of the DPA, Standard Bank will pay financial orders of US$25.2 million and will be required to pay the Government of Tanzania a further US$7 million in compensation. The bank has also agreed to pay the SFO's reasonable costs of £330,000 in relation to the investigation and subsequent resolution of the DPA.

In addition to the financial penalty that has been imposed, Standard Bank has agreed to continue to cooperate fully with the SFO and to be subject to an independent review of its existing anti-bribery and corruption controls, policies and procedures regarding compliance with the Bribery Act 2010 and other applicable anti-corruption laws. It is required to implement recommendations of the independent reviewer (Price Waterhouse Coopers LLP).

Commenting on the DPA, Director of the SFO David Green CB QC said:

"This landmark DPA will serve as a template for future agreements. The judgment from Lord Justice Leveson provides very helpful guidance to those advising corporates. It also endorses the SFO's contention that the DPA in this case was in the interests of justice and its terms fair, reasonable and proportionate. I applaud Standard Bank for their frankness with the SFO and their prompt and early engagement with us."

The suspended charge related to a US$6 million payment by a former sister company of Standard Bank, Stanbic Bank Tanzania, in March 2013 to a local partner in Tanzania, Enterprise Growth Market Advisors (EGMA). The SFO alleges that the payment was intended to induce members of the Government of Tanzania, to show favour to Stanbic Tanzania and Standard Bank's proposal for a US$600 million private placement to be carried out on behalf of the Government of Tanzania. The placement generated transaction fees of US$8.4 million, shared by Stanbic Tanzania and Standard Bank.

On 18 April 2013, Standard Bank's solicitors Jones Day reported the matter to the Serious and Organised Crime Agency and on 24 April to the SFO. It also instructed Jones Day to begin an investigation and to disclose its findings to the SFO. The resulting report was sent to the SFO on 21 July 2014.

The SFO reviewed the material obtained and conducted its own interviews. Subsequently, the Director of the SFO considered that the public interest would likely be met by a DPA with Standard Bank and negotiations were commenced accordingly.

The SFO has worked with the US Department of Justice (DoJ) and Securities and Exchange Commission (SEC) throughout this process. A penalty of $4.2m has been agreed between Standard Bank and the SEC in respect of separate related conduct.

We are very grateful to the DoJ, the SEC, the Foreign and Commonwealth Office, the Financial Conduct Authority for their assistance in resolving this investigation and deferred prosecution.

Notes for editors:

1. Please see the following documents regarding the agreement:
   Deferred Prosecution Agreement - SFO v ICBC SB PLC
   Last Updated: 18 May, 2016

   Deferred Prosecution Agreement - Statement of Facts - SFO v ICBC SB PLC
   Last Updated: 18 May, 2016

   The preliminary judgment.

   The full judgment.

2. The charge against Standard Bank has been suspended for three years, after which, subject to the bank's compliance with the terms of the DPA, the SFO will discontinue the proceedings.
3. Standard Bank's US$25.2 million total financial penalty, which is payable to HM Treasury, consists of a US$16.8 million financial penalty and a US$8.4 million disgorgement of profits. The compensation due to the Government of Tanzania consists of US$6 million, plus interest of US$1,046,196.58.
4. Standard Bank is required to pay the compensation, disgorgement of profits, financial penalty and costs within seven days of today's judgment.
5. The money due to the Government of Tanzania will be returned in line with advice being received from the Department for International Development.
6. A DPA is not a private plea "deal" or "bargain" between the prosecutor and the defendant company. It is a way in which a company accounts for its alleged criminality to a criminal court, and can have no effect until a judge confirms in open court that the DPA is in the interests of justice and that its terms are fair, reasonable and proportionate. Further information on the history of DPAs and how they are intended to be used can be found here.

Related Cases

Standard Bank PLC

HM Government

UK FINANCE

Economic Crime Plan
2019-22

July 2019

COMMISSION OF INQUIRY INTO STATE CAPTURE

© Crown copyright 2019

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications.

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gov.uk.

Contents

Foreword 2

Vision and Context 7

- Introduction 7
- What is economic crime? 10
- The threat of economic crime 11
- The economic crime response framework 13
- Our progress to date 15
- Projects and commitments 17

Strategic Priority One: Understanding the Threat and Performance Metrics 22

Strategic Priority Two: Better Information-Sharing 26

Strategic Priority Three: Powers, Procedures and Tools 32

Strategic Priority Four: Enhanced Capabilities 37

Strategic Priority Five: Risk-Based Supervision and Risk Management 47

Strategic Priority Six: Transparency of Ownership 54

Strategic Priority Seven: International Strategy 58

Governance and the public-private partnership 65

Monitoring the plan 65

Annex A – Organisations consulted in development of this plan 69

Annex B – Glossary 71

Ministerial Foreword

Economic crime is a significant threat to the security and the prosperity of the UK. It impacts all of our society, including our citizens, private sector businesses and the government. Fraud is now one of the most common crimes in the UK, with one in fifteen people falling victim a year. Money laundering enables criminals to profit from some of the most damaging crimes. Bribery and corruption undermine fair competition and are barriers to economic growth, especially in the developing world. Terrorist financing facilitates the atrocities we have suffered here in the UK as well as across Europe and the rest of the world. All economic crimes weaken people's faith in the effectiveness of governmental and commercial organisations.

To ensure the integrity of our financial system, protect our vulnerable people and communities, and attract business to the UK, we must do all in our power to combat economic crime. Last year, the Financial Action Task Force found that the UK had one of the toughest systems for combatting money laundering and terrorist financing of over 60 countries it has assessed to date. Criminals, however, are continuously adapting their methods and we know there is more work to be done.

This Economic Crime Plan represents a step-change in our response to economic crime and will lead our future response to this threat. It builds on the commitments made in the UK's 2016 Anti-Money Laundering and Counter-Terrorist Financing Action Plan, 2017 Anti-Corruption Strategy and 2018 Serious and Organised Crime Strategy to provide a collective articulation of the action being taken by the public and private sectors to ensure that the UK cannot be abused for economic crime.

The ever-evolving and clandestine nature of economic crime means it can only be combatted by harnessing the capabilities, resources, and experience of both the public and private sectors. For the first time, this plan sets out how both sectors will work together to tackle economic crime. The work of the Joint Money Laundering Intelligence Taskforce, which has so far supported over 600 law enforcement investigations, directly contributed to over 150 arrests as well as the seizure or restraint of over £34 million in illicit funds, demonstrates what a successful public-private partnership can achieve. This plan extends such public-private partnership activity to other areas in our response to economic crime.

Collectively, the actions in this plan set out an ambitious agenda to strengthen our whole-system response for tackling economic crime. A greater understanding of the threat, improved transparency of ownership, and better sharing and usage of information will enable the public and private sectors to more efficiently and effectively target their resources. They will also strengthen the resilience of the UK's defences against economic crime through enhanced management of economic crime risk in the private sector and the risk-based approach to supervision. Where criminal activity has been identified, we will have the powers and capabilities to bring the perpetrators to justice and send the message that crime does not pay. This strong domestic action will underpin our efforts to combat economic crime and illicit financial flows at the international level.

To bolster law enforcement capabilities, the government has committed over £48 million in additional funding over 2019/20. This funding will go toward the National Crime Agency's National Data Exploitation Capability and its National Assessments Centre. It will uplift investigative capability and improve capability at a local and regional level to tackle fraud. This resource will also support the continued build of the National Economic Crime Centre, which will be the national authority for the UK's operational response to economic crime, maximising the value of intelligence, and prioritising, tasking and coordinating to ensure the response achieves the greatest impact on the threat.

A key deliverable of this plan is our continued commitment to reform the suspicious activity reporting regime and the UK's Financial Intelligence Unit. As cornerstones of our whole response to economic crime, these must work better to produce richer intelligence and improve operational effectiveness. This plan also sets out our commitment to improving our response to fraud. Fraudsters are responsible for damaging the lives of a vast number of victims and we must be able to respond better to this threat.

Through this plan, the full force of both the public and private sectors will be employed to reduce the impact of economic crime felt by so many and bring to justice those criminals who act with impunity. We are resolute in our mission to protect the security and prosperity of the UK and ensure that the UK does not become a safe-haven for illicit finance. Delivering this response will ensure the UK is a world-leader in tackling economic crime.

Rt Hon Sajid Javid MP
Home Secretary

Rt Hon Philip Hammond MP
Chancellor of the Exchequer

Foreword from UK Finance

Tackling economic crime in partnership with government and law enforcement is a top priority for the finance and banking sector. As the National Crime Agency's National Strategic Assessment says – economic crime affects more UK citizens, more often, than any other national security threat. The criminals responsible exploit some of the most vulnerable in our society to scam them out of their money. They bring drugs and violence to our streets and threaten the fabric of our society. The motivation for their crime is making money. Similarly, we need to crack down on the corrupt elites who seek to hide the proceeds of corruption in the UK. That is why we regard stemming the flow of illicit finance that underpins serious and organised crime as such a high priority for the UK's banking and finance sector and it is core to the mission of the organisation I chair, UK Finance.

Simply put, we want the UK to be the safest and most transparent place in the world to conduct financial business. To achieve this will require cooperation not just within our sector, but with other key sectors, some of which are not regulated nor participating so enthusiastically in this effort today. Creating the best partnerships across government and business is the way to ensure the UK achieves our objective and continues to be a global leader in financial services. More fundamentally, it is the right thing to do for the society we serve.

We know that the partnership ethos set out in this plan can help us achieve these goals. The private sector spends billions every year fighting economic crime, often taking on responsibility for areas that have traditionally been the role of the state. We have introduced systems such as the Banking Protocol, a rapid scam-response scheme between bank branches and law enforcement, which has prevented almost £50 million of fraud and led to over 400 arrests in the past two years. And the industry sponsored a specialist police unit, the Dedicated Card and Payment Crime Unit, which prevented nearly £100 million of fraud last year and disrupted 11 organised crime gangs.

We are working with the government to deliver our Take Five to Stop Fraud campaign, helping people spot the signs of scams and protect their details and money from getting into the hands of criminals. The Joint Money Laundering Intelligence Taskforce has shown how law enforcement and the financial sector working together can develop better quality intelligence and we are supporting reform of the suspicious activity reporting regime to ensure it delivers far more effective intelligence.

But there is even more we can do and will do. The criminals behind money laundering use sophisticated techniques to target vulnerabilities in the regime. Too often we find ourselves trying to work around the limitations of the current, fragmented system. We need to move beyond operational and sectoral silos and work together in partnership to detect, disrupt and deter the criminals.

We need to develop a more comprehensive and nuanced understanding of different types of economic crime and take a more holistic and joined up approach. I believe this plan will provide the foundations for this effort and help deliver an improved way of working, including a shared understanding of threats, prioritisation and ensuring that there is the right capability and resource across the public and private sector. Given the scale of the threat, we will need to work together to ensure that our collective capability is used more effectively and that there is a proper strategic approach to tackling economic crime.

The private sector needs to play their role as good corporate citizens in supporting this plan, as this impacts all of us and the communities we live in. This is not only about sharing information but also bringing private sector expertise. We will need to innovate in the fight against economic crime, because if we do not use technology, we can be sure that the criminals will stay one step ahead. The government can support us in developing a sustainable resourcing model for economic crime reform, and by ensuring we have the right legal and regulatory frameworks to use share intelligence, data and use technology to reduce economic crime.

We and our members believe the plan and the ethos behind this plan is a positive step forward, but now we have to move into delivery and ensuring the plan is updated as threats evolve. If we do that, we can collectively help make the UK a safer and more transparent place to conduct business and a gold standard for the world in fighting economic crime.

Bob Wigley
Chairman, UK Finance

Support for the economic crime plan

This economic crime plan was commissioned by the Economic Crime Strategic Board and developed through its main working groups, the Economic Crime Delivery Board and Private Sector Steering Group. The actions contained in the plan are supported by the membership of these groups and, where relevant, the organisations responsible for the delivery of the actions.

Accountancy Affinity Group
Bank of England
Barclays
BDO LLP
City of London Corporation
City of London Police
Companies House
Consultative Committee of Accountancy Bodies
Crown Office and Procurator Fiscal Service
Crown Prosecution Service
Department of Justice, Northern Ireland
Financial Conduct Authority
Gambling Commission
Government Digital Service
HSBC
HM Courts and Tribunal Service
HM Government, led by HM Treasury and Home Office
HM Revenue and Customs
Information Commissioner's Office[1]
Institute of Chartered Accountants England & Wales
Institute of Financial Accountants
Joint Fraud Taskforce
Law Society of England and Wales
Joint Money Laundering Steering Group
Legal Sector Affinity Group
Lloyds Banking Group
Morgan Stanley
NAEA Propertymark
National Crime Agency
National Economic Crime Centre
National Police Chiefs' Council
National Terrorist Financial Investigation Unit
Nationwide
Office of Professional Body AML Supervision
Pay.UK
Payment Systems Regulator
Pensions Regulator
Police Scotland
Police Service of Northern Ireland
Public Prosecution Service for Northern Ireland
RBS
Santander UK
Scottish Government
Serious Fraud Office
Solicitors Regulation Authority
Standard Chartered Bank
UK Finance
Welsh Government

Additional private sector and civil society organisations consulted as part of the development of this plan are set out in **Annex A**.

[1] The ICO will support the Home Office and HM Treasury by attendance at the working group referred to in Action 6, in an observer capacity. ICO representatives may provide advice and guidance from a regulatory perspective, as necessary.

Vision and Context

Introduction

1.1 The UK is one of the world's leading international financial centres with a strong and open economy. The UK's standing as a global financial centre, the ease of doing business, its openness to overseas investment, status as a major overseas investor and exporter and its embrace of new and innovative technologies all create a vulnerability to economic crime. This has a significant impact on the UK's economy, competitiveness, citizens, institutions and reputation. It undermines all three of the government's national security objectives: to protect our people; to project our global influence; and to promote our prosperity.

1.2 Economic crime represents a significant threat to the UK that is ever-changing and evolving. Frequently, economic crime is serious and organised. Serious and organised crime is estimated to cost the UK at least £37 billion each year.[2] Criminality flourishes when these criminals can launder the proceeds of their illicit activity. The vast scale of money laundering in the UK represents the illicit proceeds of a range of serious crimes including large scale drug dealing and human trafficking. The volume of fraud is immense and growing. The Office of National Statistics estimated there were 3.6 million fraud offences in England and Wales in 2018 alone, with fraud accounting for almost one third of all crime experienced by individuals.[3] Terrorism can be financed through funds collected both unlawfully and lawfully. Whilst the raising and moving of funds is not a terrorist's primary aim, it may be an important enabler.

1.3 These crimes not only result in financial gain for their perpetrators, but also leave a trail of victims, causing much harm to individuals and communities and damage to legitimate business. The Home Office estimates that the social and economic cost of fraud[4] to individuals in England and Wales is £4.7 billion per year[5] and the social and economic cost of organised fraud against businesses and the public sector in the UK is £5.9 billion.[6] In 2018, UK Finance estimates that £1.2

---

[2] Home Office, The Economic and Social Costs of Crime: Second Edition, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf.

[3] Office for National Statistics, Crime in England and Wales: Additional Tables on Fraud and Cybercrime, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables.

[4] Social and economic cost calculations monetise, where possible, the full range of impacts of organised crime. This includes, where possible, costs in anticipation of crime, costs as a consequence of crime and costs in response to crime.

[5] Home Office, The Economic and Social Costs of Crime: Second Edition, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf.

[6] Home Office, Understanding Organised Crime 2015/16 0 – Estimating the Scale and the Social and Economic Costs Second Edition, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/782656/understanding-organised-crime-mar16-horr103-2nd.pdf.

billion was stolen by criminals committing authorised[7] and unauthorised fraud,[8] with the banking sector estimated to have prevented a further £1.7 billion in unauthorised fraud.[9]

1.4 Economic crime perpetrated in the UK can also undermine the security and prosperity of other countries. The UK's open economy can be abused when the proceeds of criminality overseas are laundered in the UK through the purchase of property and other assets. The reputation and ease of doing business through UK corporate structures and the UK financial system can also be abused to facilitate the laundering of criminal assets from overseas, even if this money never directly touches the UK. The government is equally determined to tackle both UK-based economic crime that directly damages our economy and society and overseas-based economic crime that undermines the integrity of the UK economy, the UK's reputation and the security and prosperity of overseas countries.

1.5 This government has made significant progress in recognising and prioritising the threat from economic crime and increasing our capability to respond to the threat. We have introduced world-leading reforms to better enable us to combat economic crime, including: the creation of the National Economic Crime Centre (NECC); establishing the Government Counter Fraud Profession; reforms to our policy and legislative framework; and the launch of dedicated public-private initiatives such as the Joint Money Laundering Intelligence Taskforce (JMLIT) and the Joint Fraud Taskforce (JFT). Since its commencement, over £1.8 billion has been taken off criminals using the powers in the *Proceeds of Crime Act 2002*, and billions more have been recovered using deferred prosecution agreements and HM Revenue and Customs' (HMRC) tax powers. Even more importantly, £293 million has been returned to victims.

1.6 Nonetheless, the threat to the UK remains high and is constantly evolving. We need to both embed the reforms we have already delivered and go further still. The wide range of individuals and organisations impacted by economic crime and its often-clandestine nature has meant that the UK's response to economic crime has been disjointed. There has been insufficient coordination and cooperation both within the public and private sectors and between the public and private sectors. There has not been a clear sense of prioritisation. This plan sets out how we can do better.

1.7 Successfully combating economic crime can only be achieved by a public-private partnership. The private sector is the first line of defence and spends substantial sums to prevent economic crime. By preventing this illicit activity from occurring in the first place, we can have a more efficient and effective response to economic crime. The private sector, particularly major financial institutions, holds significant amounts of information and data that enables law enforcement to pursue economic crime. By harnessing the capabilities, expertise and information of both the

[7] Authorised fraud, also often referred to as Authorised Push Payment (APP) scams, is where a customer is duped into authorising a payment to another account which is controlled by a criminal.

[8] In an unauthorised fraudulent transaction, the account holder themselves does not provide authorisation for the payment to proceed and the transaction is carried out by a third-party.

[9] UK Finance, Fraud the Facts 2019, https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019.

public and private sectors, we can be a world-leader in the global fight against economic crime.

1.8 To guide our collective response to economic crime, we have agreed a joint vision:

For the public and private sectors to jointly deliver a holistic plan that defends the UK against economic crime, prevents harm to society and individuals, protects the integrity of the UK economy, and supports legitimate growth and prosperity.

1.9 To deliver this vision, this plan sets out our joint response in seven priority areas that were agreed in January 2019 by the Economic Crime Strategic Board, the ministerial-level public-private board charged with setting the UK's strategic priorities for combatting economic crime. These seven priorities reflect the greatest barriers to combatting economic crime and where we see the most scope for collaborative work between the public and private sectors to improve our response.

Strategic priorities
Develop a better **understanding of the threat** posed by economic crime and our **performance** in combatting economic crime
Pursue better **sharing and usage of information** to combat economic crime within and between the public and private sectors across all participants
Ensure the **powers, procedures and tools** of law enforcement, the justice system and the private sector are as effective as possible
Strengthen the **capabilities** of law enforcement, the justice system and private sector to detect, deter and disrupt economic crime
Build greater resilience to economic crime by enhancing the **management of economic crime risk** in the private sector and the **risk-based approach to supervision**
Improve our systems for **transparency of ownership** of legal entities and legal arrangements
Deliver an **ambitious international strategy** to enhance security, prosperity and the UK's global influence

1.10 These elements are interrelated and the reform of each will improve and strengthen our overall system response to economic crime. By reforming our suspicious activity reporting (SARs) regime and the UK Financial Intelligence Unit (UKFIU), we can ensure we have the right information to combat economic crime. Through improving our understanding of the threat, powers and capabilities, we can enhance our law enforcement response to economic crime. Through enhanced risk-based supervision and private sector risk management and reforms to Companies House, we can prevent economic crimes from occurring and better enable their detection. Reforming our regime domestically gives us the platform to combat

economic crime internationally. If one area fails, it will undermine success of other areas and the effectiveness of the system as a whole.

What is economic crime?

1.11 To help establish our partnership, we have agreed a common language across the public and private sectors regarding economic crime. We have used the following definition of economic crime to guide our efforts.

Economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others. This poses a threat to the UK's economy and its institutions and causes serious harm to society and individuals. It includes criminal activity which:

- allows criminals to benefit from the proceeds of their crimes or fund further criminality;
- damages our financial system and harms the interests of legitimate business;
- undermines the integrity of the UK's position as an international financial centre; and
- poses a risk to the UK's prosperity, national security and reputation.

1.12 This definition is broader than terms such as 'financial crime'[10] or 'white-collar crime' to provide a holistic response to the following types of criminality:

- fraud against the individual, private sector and public sector;
- terrorist financing;
- sanctions contravention;
- market abuse;[11]
- corruption and bribery; and
- the laundering of proceeds of all crimes.

1.13 The recovery of criminal and terrorist assets is also in scope of this plan. Proceeds-generating crimes such as drug trafficking or human trafficking, are not covered by this plan as they are not economic crimes. However, projects relating to the laundering of the proceeds of these crimes are in scope. Projects relating specifically to tax evasion and related fiscal fraud are not in scope, except where

[10] Financial crime, for example, is defined by the *Financial Services and Market Act 2000* to include offences relating to fraud, market abuse, money laundering and terrorist financing (section 1H).

[11] For the purposes of this document, market abuse encompasses the criminal offences of insider dealing, making misleading statements and making misleading impressions.

they focus on the money laundering element of the offending.[12] While cyber-related economic crimes fall within scope of this plan, more work needs to be done on how the economic crime governance aligns with the broader cybercrime governance (see Action 50).

The threat of economic crime

1.14 Economic crime touches virtually all aspects of society. Economic crimes range across the full breadth of criminality, ranging from low-level frauds through to sophisticated cyber-enabled market manipulation. Fraud is now the second most common crime type in England and Wales, with nearly every individual, organisation and type of business vulnerable to fraudsters. While they are not victimless crimes, economic crimes such as money laundering, corruption and bribery and sanctions contravention are typically clandestine, making detection and measurement challenging. The laundering of proceeds of crime is a key enabler of most serious and organised crime impacting the UK. The threat is also continuously evolving, impacted by the emergence of new technologies, services and products such as cryptoassets.

1.15 We do not have a wholly reliable estimate of the total scale of economic crime. However, all assessments within the public and private sectors indicate that the scale of the economic crime threat continues to grow. Reported fraud is increasing in volume and remains significantly underreported. The numbers of fraud offences in England and Wales rose by 12% during 2018 alone, standing at 3.6 million – constituting a third of all crimes in the UK.[13] No reliable estimate exists for the scale of money laundering impacting the UK annually – but it is likely to be tens of billions of pounds. The challenges in distinguishing trading based on inside information or trading that is manipulative from the large volume of legitimate trading undertaken each day makes it difficult to quantify the overall scale of market abuse, although its prevalence in UK markets is not considered to be out of line with other major financial centres.

1.16 Cash-based money laundering, including through the use of money mules[14] and money service businesses, remains a significant threat. Substantial funds are also laundered via capital markets and through trade-based money laundering, reflecting the use of complex financial systems, professional enablers and insiders for high-end money laundering. Misuse of cryptoassets and alternative banking platforms are also being used to obscure ownership of assets.

1.17 The abuse of the UK financial system, corporate structures and professional services to launder the proceeds of crime from the UK and abroad continues to harm the UK's reputation. UK corporate structures are frequently misused in the most

---

[12] The government's approach to tackling tax avoidance, evasion and other forms of tax non-compliance is set out here: https://www.gov.uk/government/publications/tackling-tax-avoidance-evasion-and-other-forms-of-non-compliance.

[13] Office for National Statistics, Crime in England and Wales: Additional Tables on Fraud and Cybercrime, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables.

[14] Money mules are intermediaries for criminals and criminal organisations who, sometimes unwittingly, help to move proceeds of crime.

prominent money laundering scandals – such as those in the 'Global Laundromat' reporting. The use of UK trust and company service providers remains a key enabler of the circumvention and contravention of financial sanctions.

Professional enablers and insiders

Professional enablers can be complicit, negligent or unwitting, but are key facilitators in the money laundering process and often crucial in integrating illicit funds into the UK and global banking systems. Some types of money laundering, and in some instances the predicate offence (e.g. fraud), necessitate the services of professionals. Within the professional services sector, the criminal exploitation of accounting and legal professionals – particularly those involved with trust and company service provision – poses the greatest money laundering threat as these professionals can be used to set up corporate structures which enable high-end money laundering. Corrupt individuals, particularly those inside financial institutions, also pose a threat.

1.18 Sanctions contravention directly impacts the UK by undermining the integrity of the financial system, potentially contributing to the funding of terrorism, and to the proliferation of weapons of mass destruction. The true scale of sanctions contravention is difficult to measure and to separate from other types of financial crime. However, from April 2017 to March 2018, the Office of Financial Sanctions Implementation received 122 reports of suspected breaches of financial sanctions, with a reported value of £1.35 billion.[15]

1.19 UK contractors continue to pay bribes overseas to conduct business and improperly secure contracts. Mining and extractive industries remain those most vulnerable to bribery, in particular oil and gas. A further notable bribery and corruption risk exists in the overseas development sector, with UK contractors having paid bribes to secure development contracts. Such corrupt practices present a significant reputational risk to the UK.

1.20 Unlike most other economic crimes, the raising and moving of funds is not a terrorist's primary aim, although it may be an important enabler for their activities. There is no single typology of financial activity associated with terrorist groups or individuals. Nonetheless, terrorists depend on financial flows to self-sustain, plan and execute acts of terrorism and finance and maintain their networks. They may also rely on money to finance travel, pay for false documents, maintain safe houses, pay bribes, commit fraud, conduct training and deliver propaganda, radicalisation and recruitment campaigns. Funds for UK domestic terrorism are usually raised in small amounts often by legitimate means (e.g. salaries), but could also include fraud or other proceeds of crime.

1.21 As the UK prepares to leave the European Union, it is possible that criminals will seek to exploit changes created by the UK's departure. Without pre-emptive measures, changes affecting border controls, tariffs, trade and other economic

[15] Office of Financial Sanctions Implementation, OFSI Annual Review: April 2017 to March 2018, https://www.gov.uk/government/publications/ofsi-annual-review-april-2017-march-2018.

activity may potentially lead to an increase in the fraud and money laundering threats. The UK's departure may also affect UK businesses seeking to expand into jurisdictions beyond Europe. By engaging with new markets and industry sectors that are commonly affected by corruption, the foreign bribery threat may increase. However, through our preparations for the UK's exit, the government will ensure that criminals are prevented from taking advantage of changes.

1.22 To inform the preparation of this plan, the NCA's National Assessments Centre (NAC), supported by the NECC, led the UK's first public-private sector threat assessment of economic crime, focusing on money laundering, fraud and international bribery. This is a pilot project, from which lessons learned and best practices will be drawn to inform the UK's response to serious and organised economic crime. The threat assessment highlighted several areas of particular concern across both sectors, including:

- the need for more information and intelligence sharing;
- the use of money mules and their recruitment via social media;
- the threat from corrupt professional enablers and insiders;
- the role of technology and innovation in addressing or creating new threats; and
- the abuse of corporate structures.

1.23 The response to these threats is set out in the plan. As part of its role bringing together the overall response to serious and organised economic crime, the NECC will ensure the findings of the first public-private threat update are reflected in law enforcement's operational response (see Action 21).

The economic crime response framework

1.24 The government's response to economic crime is led by HM Treasury and the Home Office, with key responsibilities also held by the Department for Business, Energy and Industrial Strategy, the Ministry of Justice, the Attorney General's Office, the Cabinet Office, the Department for International Development, the Foreign & Commonwealth Office (FCO) and many others. The Scottish Government is responsible for criminal justice policy in Scotland. In Northern Ireland, criminal justice policy is overseen by the Department of Justice. More detail on the agencies and organisations involved in tackling economic crime is set out in **Annex B.**

1.25 The NCA leads and co-ordinates the response to serious and organised crime in England and Wales and hosts the UKFIU, the NECC and the NAC. The NECC is a collaborative, multi-agency centre that was established on 31 October 2018 to deliver a step-change in the response to tackling serious and organised economic crime. The NECC brings together law enforcement agencies, including the NCA, Serious Fraud Office (SFO), HMRC, Financial Conduct Authority (FCA), Crown Prosecution Service (CPS) and the City of London Police as the national police lead for fraud in England and Wales. It also houses government departments, regulatory bodies and the private sector to create a shared objective of driving down serious and organised economic crime across the whole community. The NECC will work in partnership with the 43 English and Welsh police forces and the nine Regional Organised Crime Units, as well as Action Fraud and the National Fraud Intelligence

Bureau hosted in the City of London Police. The Metropolitan Police Service host the National Terrorist Financial Investigation Unit, which is the UK's strategic operational lead for terrorist finance.

1.26 The policing response to serious and organised crime is a devolved matter. In Scotland, the Crown Office and Procurator Fiscal Service, which operates under the authority of the Lord Advocate, is the sole prosecuting authority, responsible for the investigation and prosecution of crime.[16] Police Scotland is the single police force in Scotland, and works closely with the NCA, HMRC, the FCA and other relevant agencies in investigating economic crime. The Scottish Crime Campus is a multi-agency centre, established by the Scottish Government in 2015, which accommodates the key agencies involved in tackling economic crime in Scotland.

1.27 The Police Service of Northern Ireland is the lead operational agency for serious and organised crime in Northern Ireland and the NCA and other UK law enforcement agencies work closely with them. The Public Prosecution Service for Northern Ireland is the prosecuting authority.

1.28 The UK has 25 anti-money laundering and counter-terrorist financing (AML/CTF) supervisors appointed by HM Treasury under the *Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017* (MLRs). There are three statutory supervisors, the FCA, HMRC and the Gambling Commission, and 22 professional body accountancy and legal supervisors. The Office for Professional Body AML Supervision is an oversight body for the legal and accountancy professional body supervisors. The Office of Financial Sanctions Implementation helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom.

1.29 The Cabinet Office leads the public sector response to fraud. It has invested in developing the evidence base for public sector fraud, including estimates of the level of fraud loss. These are published every year in the government's Fraud Landscape Report.[17] In addition, it has set out the basics that all public bodies should have in place to deal with fraud and economic crime, and publishes departmental compliance with this every year. In 2018, the government launched the Government Counter Fraud Profession for those working in the public sector to fight fraud. Through this, the Cabinet Office is transforming capability across government to enable public bodies to better fight economic crime.

1.30 The private sector organisations involved in our response to economic crime are even more diverse, in terms of numbers, capabilities and roles. While all private sector organisations may be vulnerable to economic crime, key stakeholders for the plan include those businesses with obligations under the MLRs, such as those within the banking, finance, money service, accountancy, legal and real estate sectors ('regulated firms'), and sectors engaged in the delivery of certain elements to tackle fraud, such as telecommunications.

---

[16] The responsibilities of the Lord Advocate and the Crown Office and Procurator Fiscal Service apply to crimes which are reserved (e.g. money laundering) and to crimes which are devolved (e.g. fraud, embezzlement, bribery).

[17] Cabinet Office, Cross-Government Fraud Landscape Annual Report 2018, https://www.gov.uk/government/publications/cross-government-fraud-landscape-annual-report-2018.

1.31 The UK's current response to economic crime includes several collaborative public-private partnerships targeting specific economic crime threats. This includes JMLIT, the JFT and the Dedicated Card and Payment Crime Unit (DCPCU). As detailed below, these partnerships have led to real results in combatting economic crime.

Results delivered through public-private partnership work

Joint Money Laundering Intelligence Taskforce

- Established in 2015 to exchange and analyse financial information relating to money laundering and other economic crime threats.
- Hosted by the NCA, it consists of 40 financial institutions, HMRC, SFO, City of London Police, the Metropolitan Police Service, the FCA, and Cifas.
- Since its inception, JMLIT has supported and developed over **600 law enforcement** investigations which have directly contributed to over **150 arrests** and the seizure or restraint of over **£34 million**.

Joint Fraud Taskforce

- The JFT is a partnership between banks, law enforcement and government to deal with fraud.
- JFT continues to build on successful initiatives such as the **banking protocol**, which is a partnership between UK Finance members and policing. The JFT has supported the roll-out of this initative to all 45 territorial police forces. It has prevented over **£48 million** from falling into fraudsters' hands and has led to over **400 arrests** since its introduction in October 2016.

Dedicated Card and Payment Crime Unit

- The DCPCU is fully sponsored by the banking industry and works to identify and target the organised crime groups responsible for card and payment crime.
- It is a partnership between City of London Police, the Metropolitan Police Service, UK Finance and the Home Office.
- DCPCU prevented an estimated **£94.5 million** of fraud in 2018: a new record high. This brings the unit's total estimated savings from reduced fraud activity to **£600 million** since it was established in April 2002.

Our progress to date

1.32 The government published the Serious and Organised Crime Strategy in November 2018.[18] Scotland and Northern Ireland have also published their own respective strategies.[19] In alignment with the UK's Serious and Organised Crime Strategy, this plan sets out the collective response of the public and private sectors against economic crime specifically.

1.33 The plan also sits alongside the 2017 Anti-Corruption Strategy.[20] Although it does not seek to duplicate actions in that Strategy, it is complementary and seeks to support a number of the same approaches including working with international partners and protecting the UK as a leading financial centre. Given the government's commitment to drive up the recovery of proceeds of crime in relation to all criminality,

---

[18] Home Office, Serious and Organised Crime Strategy 2018, https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2018.

[19] Scottish Government, Serious Organised Crime Strategy 2015, https://www.gov.scot/publications/scotlands-serious-organised-crime-strategy/; Organised Crime Task Force, The Northern Ireland Organised Crime Strategy 2016, https://www.octf.gov.uk/Publications/N-I-Organised-Crime-Strategy.

[20] Department for International Development and the Home Office, UK Anti-Corruption Strategy 2017-2022, https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022.

the 2019 Asset Recovery Action Plan is published alongside this plan. It sets out the actions that are being taken forward to fulfil the government's ambition of seeing a return to year on year increases in the recovery of criminal property and assets.[21]

1.34 The plan incorporates our response to several recent reports. It builds on the government's 2016 AML/CTF Action Plan.[22] The 2016 action plan led to a number of reforms to the UK's AML/CTF regime, which was evaluated in 2018 by the Financial Action Task Force's (FATF) mutual evaluation report (MER).[23] Altogether, the findings of the MER showed that the UK has the strongest overall AML/CTF regime of over 60 countries assessed to date. In particular, the MER praised the UK's understanding of risk, response to terrorist financing and our targeted financial sanctions regime. The MER also underlines the importance of our ongoing efforts to develop the UK's AML/CTF regime, particularly in relation to the UKFIU and the SARs regime, AML/CTF supervision, industry implementation of AML/CTF obligations and Companies House reform. Similar findings were made in the Treasury Select Committee's report on its inquiry into economic crime, which was published on 8 March 2019.[24]

1.35 The UK also underwent a review of its compliance with the United Nations Convention against Corruption (UNCAC) in 2017/18, focusing on prevention of corruption (including money laundering) and asset recovery.[25] Overall, the UK received a positive review from the UNCAC reviewers. UNCAC issued ten recommendations and this plan will address those on the evidence base of corruption, SARs, asset recovery and money laundering. The government response to the other recommendations will be addressed separately as part of the government's implementation of the Anti-Corruption Strategy.

1.36 In March 2019, the UK updated the Organisation for Economic Co-operation and Development (OECD) Working Group on Bribery on the implementation of the recommendations contained in the UK's 2017 Phase 4 review of the OECD Anti-Bribery Convention. The UK provided a two-year update which outlined the significant progress against many of the key recommendations for the UK such as enhancing law enforcement co-operation and engagement with the private sector. The UK received a favourable review from the OECD and will work to implement the outstanding recommendations before its next update in March 2021. In the same month, the House of Lords Bribery Act Committee recommended the *Bribery Act*

---

[21] Home Office, Asset Recovery Action Plan, https://www.gov.uk/crime-justice-and-law/crime-prevention.

[22] HM Treasury and Home Office, Action Plan for Anti-Money Laundering and Counter-Terrorist Finance, https://www.gov.uk/government/publications/action-plan-for-anti-money-laundering-and-counter-terrorist-finance.

[23] Financial Action Task Force, Mutual Evaluation Report of the United Kingdom, http://www.fatf-gafi.org/countries/u-z/unitedkingdom/documents/mer-united-kingdom-2018.html.

[24] Treasury Select Committee, Economic Crime – Anti-Money Laundering Supervision and Sanctions Implementation, https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/inquiries1/parliament-2017/economic-crime-17-19/.

[25] United Nations Office on Drugs and Crime, Country Review Report of the United Kingdom, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778366/UK_Final_country_review_report_18.3.2013.pdf.

2010 as an exemplary piece of anti-corruption legislation.[26] The recommendations made in their final report cover issues such as improving awareness of the Act and its accompanying guidance amongst small and medium enterprises.

1.37 In April 2019, Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) released its report on the police response to fraud in England and Wales. It found that although the current fraud policing model of local and regional investigations supported by national functions is the right one, significant improvements are required to ensure it works more effectively and efficiently.[27]

1.38 Where appropriate, this plan incorporates our response to the recommendations from these reports.

Projects and commitments

1.39 To develop this plan, representatives from the public and private sectors have worked together to identify threats and agree the ambition of our collective response to tackle these threats. As detailed in **Table 1,** we have set ourselves a set of ambitious targets, which we will seek to deliver under best endeavours. We do not underestimate the challenges of doing so given the ever-evolving threat of economic crime, the complexities of the issues we are seeking to resolve, and the unique way of working that we are pursuing through this public-private partnership.

1.40 Some of the actions in this plan are aimed at targeting economic crime holistically, while others are focused on specific threats, particularly money laundering and fraud. There is substantial work to be done to ensure the policy and operational response to money laundering and fraud are appropriately linked, as they often deal with similar issues but have different corporate histories, governance, stakeholders and information-sharing arrangements. This is not to minimise the importance of the UK's response to other economic crime threats. For crimes such as terrorist financing and sanctions contravention, the FATF found the UK's existing policy and operational response was highly effective with only minimal reforms necessary. For bribery and corruption, a large body of work aimed at enhancing the UK's response is being led through the implementation of the 2017 Anti-Corruption Strategy.

The private sector will be heavily involved in helping deliver the plan. In agreeing the organisations responsible for leading on actions however, there are challenges in reflecting all the firms involved. Given this is a new way of working and the breadth of firms in the private sector, it is not possible to easily list all the parts of the private sector involved. We have sought, wherever possible, to use relevant industry bodies to indicate the parts of the private sector most directly involved. In addition, the representative private sector bodies named in the plan have agreed to work together to develop governance and mechanisms for regulated firms that will allow them to engage and convene their members to support the plan.

---

[26] Bribery Act 2010 Committee, The Bribery Act 2020: Post-Legislative Scrutiny, https://www.parliament.uk/business/committees/committees-a-z/lords-select/bribery-act-2010/news-parliament-2017/bribery-act-2010-report-publication/.

[27] Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services, Fraud: Time To Choose, https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf.

Table 1: Agreed actions for economic crime plan

Action	Responsible organisation(s)	Due date
Understanding the threat and performance metrics		
1. Undertake collective threat assessments	NAC with support of NECC, UK Finance, Legal Sector Affinity Group (LSAG), Accountancy Affinity Group (AAG), HM Treasury (HMT), Home Office	Ongoing
2. Develop a fully operational performance system to measure what works	Home Office, UK Finance, NECC, JFT	July 2020
3. Conduct new National Risk Assessments on money laundering, terrorist financing and proliferation financing	HMT, Home Office	July 2020
4. Better understand the threat and performance in combatting public sector fraud	Cabinet Office	Ongoing
5. Resolve evidence gaps through a long-term research strategy	Home Office, with support of NECC, HMT, Ministry of Justice	December 2019
Better information-sharing		
6. Review barriers to information-sharing, powers and gateways	Home Office, HMT, with support of NECC, UK Finance, Information Commissioner's Office,[28] LSAG, AAG, Department for Digital, Culture, Media and Sport	March 2020
7. Promote sharing of information in corporate groups	Home Office, HMT	March 2020
8. Expand and enhance public-private information-sharing through JMLIT	NECC, HMT	July 2020
9. Improve information-sharing between AML/CTF supervisors and law enforcement	NECC, UKFIU, OPBAS, with support of AML/CTF supervisors, LSAG, AAG	Ongoing
10. Promote information-sharing in relation to fraud	Home Office, Cabinet Office	December 2020
Powers, procedures and tools		
11. Implement the Asset Recovery Action Plan	Home Office, law enforcement agencies	July 2022

[28] The ICO will attend the working party in an observer capacity. ICO representatives may provide advice and guidance from a regulatory perspective as necessary

Action	Responsible organisation(s)	Due date
12. Consider legislative changes to improve the Proceeds of Crime Act	Home Office	December 2021
13. Transpose the Fifth Money Laundering Directive	HMT	January 2020
14. Implement the Disclosure Review recommendations	AGO, CPS, NPCC	December 2019
15. Consider tactical targeting orders	Home Office, HMT, UKFIU	July 2020
16. Develop framework to repatriate funds to victims of fraud	Home Office, with support of JFT, UK Finance	December 2021
17. Clarify sanctions supervision powers	HMT, with support of AML/CTF supervisors, LSAG, AAG	July 2020
18. Review the criminal market abuse regime	FCA, HMT	July 2021
19. Investigate power to block listings on national security grounds	HMT	June 2020
Enhanced capabilities		
20. Continue to develop the NECC as a genuine public-private hub for combatting serious and organised economic crime	NECC	July 2021
21. Understand and enhance capabilities	NECC, Cabinet Office, UK Finance	July 2020
22. Develop public-private action plans to combat economic crime threats	NECC, Home Office, HMT, UK Finance	January 2020
23. Develop a sustainable, long-term resourcing model for economic crime reform	Home Office, with support of HMT, NCA, UK Finance, Cabinet Office	March 2020
24. Launch flagship economic crime court in central London	HM Courts and Tribunal Service, Ministry of Justice, with support of City of London Corporation	Ongoing
25. Consider how the payments systems can help tackle economic crime	Pay.UK, with support of Payment Systems Regulator, FCA, HMT, UK Finance; Bank of England	2021
26. Improve the policing response to fraud	Home Office, with support of City of London Police, NECC	March 2020
27. Improve support for victims of fraud	Home Office	August 2020
28. Close the vulnerabilities that criminals exploit to conduct fraud	JFT	December 2020

Action	Responsible organisation(s)	Due date
29. Build our Government Counter Fraud Profession	Cabinet Office	April 2021
30. Deliver first tranche of SARs IT transformation and design the target operating model for the future of the SARs regime	SARs Transformation Programme, NCA, Home Office, with support of HMT	December 2020
31. Deliver greater feedback and engagement on SARs	SARs Transformation Programme, UKFIU, Home Office	2020
32. Ensure the confidentiality of the SARs regime	Home Office, UKFIU, with support of HMT	December 2019
Risk-based supervision and risk management		
33. Review the MLRs and OPBAS regulations	HMT	June 2022
34. Enhance FCA supervision and engagement	FCA, with support of Pensions Regulator	March 2021
35. Enhance HMRC supervision	HMRC, with support of OPBAS, HMT	March 2021
36. Strengthen the consistency of professional body AML/CTF supervision	OPBAS, accountancy and legal professional body supervisors	March 2021
37. Establish the FCA as the supervisor of the future cryptoassets AML/CTF regime	FCA	January 2020
38. Support innovation in regulatory compliance for AML/CTF	FCA, HMT, UK Finance with the support of Home Office, Corporation of the City of London	Ongoing
39. Enhance firms' holistic response to economic crime	UK Finance, with support of other relevant industry associations	Ongoing
40. Promote digital identity services	HMT, with support of the Digital Identity Unit, Joint Money Laundering Steering Group, HMRC, Gambling Commission, LSAG, the Consultative Committee of Accountancy Bodies	October 2019
41. Education and awareness-raising on economic crime threats and the recovery of criminal assets	NECC, UK Finance, Home Office with support of LSAG, AAG	December 2019
Transparency of ownership		
42. Reform Companies House	BEIS, with support of Companies House	Ongoing

Action	Responsible organisation(s)	Due date
43. Introduce a requirement to report discrepancies of beneficial ownership information	HMT	January 2020
44. (i) Enhance transparency of overseas ownership of UK property and (ii) reform limited partnerships	(i) BEIS, with support of Companies House (ii) BEIS	(i) 2021 (ii) Ongoing
International strategy		
45. Improve understanding of the nature and impact of the international threat	NECC, UKFIU, Home Office, DFID	Ongoing
46. Joint work on meeting international standards	Home Office, HMT, UK Finance, DFID, with support from Corporation of the City of London, FCO, Government Digital Service	Ongoing
47. Enhance overseas capabilities	DFID, International Centre of Excellence, Home Office, DFID, FCO, FCA, HMRC, Gambling Commission, HMT, OPBAS, NECC, UKFIU, Cabinet Office	Ongoing
48. Strengthen capability to investigate and prosecute bribery and corruption overseas	DFID, NCA, CPS, FCO	Ongoing
49. Promote integrity in business internationally	DFID, Department for International Trade, FCO, with support from Corporation of the City of London	Ongoing until 2021
Governance and public-private partnership		
50. Review the economic crime governance	Home Office, HMT	September 2019
51. Develop stronger public-private and private-private partnerships	Home Office, HMT, UK Finance with support from LSAG, AAG, Corporation of the City of London	Ongoing
52. Enhance engagement with civil society	Home Office, HMT	Ongoing

Strategic Priority One: Understanding the Threat and Performance Metrics

Objective

Develop a better understanding of the threat posed by economic crime and our performance in combatting economic crime

Introduction

2.1 The clandestine nature of most economic crimes presents substantial challenges in developing an effective response. Economic crimes can involve complex methodologies that are continuously changing as criminals and terrorists identify and exploit new vulnerabilities in society. Accordingly, we must have a comprehensive and up-to-date understanding of the threat of economic crime. A better understanding of the threat plays a key role in enabling the public and private sectors to collectively prioritise the policy reforms and operational activity that deliver the highest impact in combatting economic crime.

2.2 The UK conducts a range of threat and risk assessments to develop our understanding. The 2016 AML/CTF Action Plan made closing intelligence gaps a priority. The NCA's National Strategic Assessment assesses the economic crime threats facing the UK on an annual basis.[29] As required under the MLRs, the UK also conducts periodic national risk assessments (NRAs) of money laundering and terrorist financing, which provide an overview of the risks and likelihood of an activity occurring.[30] The NRA is the definitive high-level assessment of money laundering and terrorist financing risk in the UK. AML/CTF supervisors and regulated firms must take NRAs into account when conducting their own risk assessments of the specific money laundering and terrorist financing risks faced by their sectors or business. Agencies, including the NCA, HMRC, SFO, FCA and policing, also conduct their own sectoral and threat-focused assessments on economic crime.

2.3 Despite this ongoing work, gaps remain in our current collective understanding of the threat of economic crime. To address this, we will take a strategic approach to address gaps in our evidence base for different types of economic crimes and limitations in the data and statistics we collect. In 2019, the National Assessments Centre conducted the first formal public-private economic

[29] National Crime Agency, National Strategic Assessment of Serious and Organised Crime 2019, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file.

[30] HM Treasury and Home Office, National Risk Assessment of Money Laundering and Terrorist Financing 2017, https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017.

crime threat assessment and this process will be built upon in the future. We will expand our NRAs to include a wider range of economic crimes by producing our first ever NRA on proliferation financing. We will also continue work to better understand the threat of public sector fraud and ensure public sector organisations develop risk assessments of the fraud risks that they face.

2.4 We also need to ensure that we can measure the impact of our collective actions to tackle economic crime through a more rigorous framework for measuring performance. By improving our collective understanding of the threat and our performance, we can better ensure that our operational and policy response to economic crime is targeted at the highest priority threats and that we are prioritising the most effective tools.

The public-private partnership

2.5 There is substantial scope for greater public-private collaboration in understanding the threat of economic crime. The public and private sectors are already producing joint threat assessments on economic crime. Having analysts from the public and private sectors sharing knowledge and expertise allows a much more comprehensive and nuanced understanding of the threat. A better understanding of the threat ensures that both sectors are able to better identify illicit activity and ensure that activity is focused on the highest priority threats. This improves the preventive measures the private sector deploys to stop crime in the first place, as well as enhancing the law enforcement response. Measuring performance will also help demonstrate what actions have the greatest impact in combatting economic crime.

Projects and Commitments

Action 1: Undertake collective threat assessments

2.6 The **NAC,** supported by the **NECC, UK Finance,** the **Legal Sector Affinity Group (LSAG)**, **Accountancy Affinity Group (AAG)** and other public and private sector partners, will build on the first public-private threat update by undertaking further joint strategic assessments on economic crime. Updates on the overall serious and organised economic crime threat will be supported by a programme of regular and more detailed thematic and sectoral assessments focused on specific areas of economic crime which may benefit from joint analysis, such as the property sector or high-risk jurisdictions. The thematic assessments will further improve the evidence base upon which NRAs are conducted.

2.7 For the system to work effectively, our operational understanding of the threat needs to consistently inform the government's policy response and the approach of regulators. **HM Treasury** and **Home Office** will establish a quarterly forum to consider the policy implications of the latest understanding of the threat arising from the work detailed above. The first forum will be held by September 2019.

Action 2: Develop a fully operational performance system to measure what works in combatting economic crime

2.8 To fully measure the efforts in the public and private sectors in disrupting economic crime, the **Home Office** will lead an outcome-based approach and develop performance indicators to monitor activities being undertaken to tackle economic crime. A baseline will be in place by December 2019 and the performance system will be fully operational by July 2020. **UK Finance** will lead other relevant industry bodies in developing performance indicators for the private sector.

2.9 Performance work will involve mapping data which is already collected and held by the public and private sectors, leveraging pre-existing work to obtain information from agencies and considering 'what good looks like' and 'what works' in combatting economic crime. The **NECC** will lead on collecting performance data from law enforcement for serious and organised economic crime, and the **JFT** will develop a performance framework to understand what actions are having the greatest impact on fraud reduction.

Action 3: Conduct new National Risk Assessments on money laundering, terrorist financing and proliferation financing

2.10 **HM Treasury** and **Home Office** will lead the production of a third NRA on money laundering and terrorist financing by July 2020. The public-private threat assessments outlined in Action 1, including more detailed sectoral assessments, will further enrich the evidence base for future NRAs. HM Treasury and Home Office will continue to enhance the transparency of the NRA methodology to ensure the NRA's conclusions are widely understood and accepted.

2.11 Following the 2015 Strategic Defence and Security Review[31] and development of the National Counter-Proliferation Strategy 2020, combating the financing of the proliferation of weapons of mass destruction has been at the centre of the UK's broader counter-proliferation efforts.

2.12 The UK's status as a global financial and insurance centre with significant cross-border linkages, means that it continues to face a wide range of proliferation financing risks. **HM Treasury** will therefore lead the production of the UK's first NRA on proliferation financing for release by July 2020.

Action 4: Better understand the threat and performance in combatting public sector fraud

2.13 In the public sector, the **Cabinet Office** will work with government departments and arms-length bodies to help them continue to develop fraud risk assessments that detail the risks they face, as part of their work to meet the Counter Fraud Functional Standard. Government departments and arms-length bodies will continue to develop and deliver annual action plans, detailing activity each year to

[31] HM Government, National Security Strategy and Strategic Defence and Security Review 2015, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

develop their counter fraud and economic crime response. Alongside these, they will develop outcome-based metrics demonstrating their performance and impact.

Action 5: Resolve evidence gaps through a long-term research strategy

2.14 An important part of building our capacity to respond is improving our evidence base. Good quality and robust research is fundamental to ensuring a comprehensive understanding of the threat and the most effective and efficient targeting of resources. To this end, the **Home Office**, working with the **NECC** and other key partners, will produce a long-term research strategy by December 2019, setting out the key evidence gaps in our understanding of the threat from economic crime.

2.15 This long-term research strategy will seek to map existing work that is being planned or carried out by key partner agencies; prioritise evidence gaps which will deliver the greatest value-add in our understanding of the threat; and, will focus on improving our awareness of the nature, extent, and threat of various types of economic crime. Developing the evidence base cannot be achieved by government or law enforcement alone. We will work with partners from academia, industry and elsewhere to tackle the research questions that most clearly support implementation of this action.

2.16 The strategy will include policy work, led by the Home Office in conjunction with **HM Treasury** and the **Ministry of Justice**, to review whether the statistics that are collected on economic crime, particularly criminal justice statistics, can be improved. This should consider the FATF MER's recommendations on the collection of statistics under the UK's AML/CTF regime and the UNCAC review's recommendation on developing a better understanding of the threat posed by domestic corruption.

INTO STATE CAPTURE

Strategic Priority Two: Better Information-Sharing

Objective

Pursue better sharing and usage of information to combat economic crime within and between the public and private sectors across all participants

Introduction

3.1 The increasing digitisation of society has led to ever growing amounts of data which can help identify economic crimes and criminal activity. However, our response to economic crime is spread across a myriad of public and private sector organisations, meaning that information is siloed and segmented between different organisations and even within organisations themselves. This presents a fundamental challenge for organisations to understand and respond to the threat posed by economic crime. Criminals and terrorists ruthlessly exploit this information asymmetry to hide their ill-gotten gains and prevent their criminality from being exposed.

3.2 No one agency or organisation has the information, intelligence or data necessary to combat economic crime alone. This can only be achieved by agencies and organisations having the appropriate powers, gateways, frameworks and culture in place to facilitate the effective, appropriate and targeted sharing and use of information. By bringing together and analysing the information held by separate organisations, through multi-agency partnerships such as the NECC, we can better target and mitigate our economic crime threats. The private sector can better devote their resources to addressing the most important risks and providing higher quality intelligence to the public sector. The public sector can undertake better cross-system analysis of intelligence to disrupt economic crime and providing better quality guidance back to the private sector on threats. Through the mutual sharing of information, criminals and terrorists can be identified and held to account and the proceeds of their crime can be traced and returned to their victims. This increases our ability to prevent and deter further offending and to protect our country and society from economic crimes.

3.3 The UK has been a world-leader in promoting the appropriate sharing and use of information on economic crime. The establishment of the JMLIT as an operational pilot in 2015 has led to a paradigm shift in how financial intelligence can be exchanged and analysed and several other countries have now established their own public-private information-sharing platforms. The JMLIT operates on both a tactical level, through its operations group, and at a strategic level, through Expert Working Groups, which focus on key priority areas such as bribery and corruption, trade-based money laundering, terrorist financing and money laundering through capital markets.

3.4 We have also introduced major recent legislative reforms intended to clarify information-sharing requirements and facilitate information-sharing to tackle economic crime, including the *Criminal Finances Act 2017* and the *Data Protection Act 2018*, which permits the processing of personal data where it is necessary for the purposes of the prevention of crime, subject to certain safeguards. As detailed in Action 30, we also have an ambitious programme to transform the UK's SARs regime and the UKFIU.

3.5 However, much more can be done to promote better quality information-sharing and use to combat economic crime. Barriers remain to information-sharing and valuable intelligence is being lost in silos between and within organisations. The actions in this chapter set out our collective ambition for the right organisations to have access to the right information at the right time, with the appropriate structures, controls and culture in place to facilitate this.

3.6 When information being shared consists of personal data, such sharing, whether between or within the public and private sectors, must comply with data protection legislation (the *Data Protection Act 2018* and *Regulation (EU) 2016/67 – the General Data Protection Regulation)* and the Information Commissioner's Office's (ICO) data-sharing code of practice.[32] This is to ensure that the rights of data subjects are protected and their privacy is respected. People want and expect law enforcement agencies and private sector firms to stop economic crime, but they also want to know how and why their information is being used. They want to know that it is used responsibly and kept safely, and that they have redress where there is misuse.

3.7 There needs to be a sustained focus to identify where barriers to appropriate information-sharing on economic crime lie, whether domestic or international. We need to consider how appropriate information-sharing can be enhanced, including through development of guidance, raising awareness of existing gateways, and, where necessary, legislation. This includes considering the regulatory expectations, operational infrastructure, cost involved and culture around information-sharing, as well as concerns relating to data protection, privacy, commercial aspects, anti-competitive behaviour, client confidentiality and privilege.

3.8 The barriers are potentially different where it is 'voluntary' or 'permissive' information-sharing. Unlike 'mandatory' information-sharing, such as the SARs regime, there is not a clear obligation on a party to share information. Voluntary information-sharing is not a substitute for the SARs regime, but can be a valuable complement, by assisting in the development of higher quality SARs to the UKFIU in certain circumstances. These barriers are also different when sharing information internationally as opposed to domestically. Improving cross-border information sharing in both the public and private sectors will enable a more thorough understanding of risk, trends and methodologies in relation to economic crime and enable both the public and private sectors to better target their efforts.

3.9 Informed by this work, we will release clear statements on our expectations on information-sharing in corporate groups, similar to those issued by the Monetary

[32] The ICO's data-sharing code is being updated to reflect the new legislation. The current version is available on the ICO's website: https://ico.org.uk/.

Authority of Singapore.[33] We will also continue to build on the success of JMLIT and enhance its operations, as well as improve our ability to share information relating to fraud, including through the Counter Fraud Data Alliance.

The public-private partnership

3.10 We see substantial opportunity to use public-private partnerships as mechanisms to improve the sharing of information and intelligence between the public and private sectors, as well as promoting collaboration within the private sector. As set out in the Asset Recovery Action Plan (see Action 11), the private sector's expertise should be harnessed to enrich data and assist in the identification and recovery of proceeds of crime. We should build on the success of platforms such as JMLIT and take learning from these initiatives to overhaul our wider joint approach to information-sharing. This includes reforming the SARs regime to facilitate better sharing and exploitation of data. Working groups with mixed public and private representation will help ensure our legislation and guidance enables information-sharing and does not inhibit it unnecessarily.

Projects & Commitments

Action 6: Review barriers to information-sharing, powers and gateways

3.11 **Home Office** and **HM Treasury,** with support from **NECC**, **UK Finance, ICO,**[34] **LSAG** and **AAG,** will establish a public-private working group with public and cross-sectoral private sector representatives focused on information-sharing for economic crime purposes by July 2019.

3.12 The group will review the UK's existing information-sharing framework for economic crime, including information-sharing between and within public and private sectors, within corporate groups and the sharing of information domestically and internationally. This review will focus on:

- mapping current gateways, powers and information-sharing partnerships and considering whether they are appropriate, clearly defined and universally interpreted;
- identifying what barriers exist and whether these barriers are legal, arising from regulatory expectations, technical, financial and/or cultural;
- whether there are public datasets that can be used by the private sector to improve their risk understanding, as well as developing a better understanding of what data is available in the private sector that could be

[33] Monetary Authority of Singapore, FATF Guidance on Private Sector Information Sharing and revised INR.18, http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Guidance-Papers/2018/FATF-Guidance-on-Private-Sector-Information-Sharing-and-Revised-INR18.aspx.

[34] The ICO will attend the working party in an observer capacity. ICO representatives may provide advice and guidance from a regulatory perspective as necessary.

used by law enforcement to develop a more sophisticated understanding of threat (see Action 5);

- whether gateways are sufficient for the sharing of information between private sector organisations, particularly sharing to enable them to fulfil their regulatory obligations (e.g. in fulfilling customer due diligence obligations under the MLRs);
- whether there are sufficient standards around how and what information is shared between the public and private sectors (e.g. information shared by the private sector for intelligence or evidential purposes);
- ways in which the cross-border sharing of information can be promoted, including consideration of bilateral reciprocal arrangements for sharing information with full regard given to existing cross-border information-sharing networks such as the Egmont Group's principles for FIUs;[35]
- considering the potential 'derisking' implications that could arise from greater information-sharing and how to ensure the sharing of information does not give one organisation an unfair advantage; and
- considering the ethical implications relating to any information-sharing reforms, including what governance structures need to be put in place that would afford ethical decision-making.

3.13 The review should result in a report by March 2020 setting out recommended actions for reform and should aim to establish the UK as a world-leader in promoting the appropriate and proportionate sharing and use of high-quality information for economic crime purposes. The group will ensure that, where the barriers are cultural, all parties work towards a solution to make best use of the current gateways to address economic crime. The group will ensure that its recommendations will complement the SARs Transformation Programme (see Action 30) and ongoing work of the JFT. The review will also inform and draw upon the work of the **Department for Digital, Culture, Media and Sport** to develop the UK's National Data Strategy.[36]

Action 7: Promote sharing of information in corporate groups

3.14 Through the information-sharing working group, the **Home Office** and **HM Treasury** will, by March 2020, release a statement setting out the government's expectations on information-sharing within corporate groups and between different business units within corporates for economic crime purposes. This should set out a clear statement from the government on the ability of corporates to share information within their groups and firm, both domestically and cross-border. This will help ensure that firms' determination of risk encompasses global considerations and be used as a basis to promote greater international consistency in cross-border information-sharing.

[35] Further information is available on the Egmont Group's website: https://egmontgroup.org//.

[36] Department for Digital, Culture, Media & Sport, National Data Strategy Open Call For Evidence, https://www.gov.uk/government/publications/national-data-strategy-open-call-for-evidence/national-data-strategy-open-call-for-evidence.

3.15 Following the review on information-sharing, further clarificatory statements may be released.

Action 8: Expand and enhance public-private information-sharing through JMLIT

3.16 Informed by the work of the information-sharing working group, the **NECC** will lead the enhancement of JMLIT by July 2020, building on its strengths and the characteristics that make it function effectively. This will include consideration of:

- how the JMLIT should expand to include additional sectors, geographical areas and additional organisations within sectors currently included in JMLIT, recognising that different sectors will have different intelligence-sharing needs and capabilities;
- how JMLIT can improve collaboration between sectors;
- how to better disseminate information to firms and sectors which are not part of JMLIT, including lessons learned, typologies and trends;
- how JMLIT works alongside other information-sharing arrangements, the UKFIU, and the SARs Transformation Programme (see Action 30);
- the technology supporting JMLIT and how to promote data standardisation, including through guidance and templates on how JMLIT members should respond to a JMLIT request; and
- ensuring that the JMLIT's Expert Working Groups maximise the sharing of the strategic understanding of the threat to feed into future threat reporting.

3.17 As part of this work, the **NECC,** with support from **HMT**, will conduct an international information-sharing pilot linking up JMLIT with foreign public-private partnerships by July 2020. This should be done on a bilateral and multilateral basis with other financial centres, cognisant of pre-existing international information-sharing frameworks such as the exchange of financial intelligence through the Egmont Group.

Action 9: Improve information-sharing between AML/CTF supervisors and law enforcement

3.18 As informed by the SARs Transformation Programme, **NECC** and **UKFIU,** working with the **AML/CTF supervisors,** will promote the legitimate, appropriate and proportionate sharing of information between law enforcement and AML/CTF supervisors. Building on existing UKFIU referral processes, this will consider what SAR information can be shared, including in respect of weaknesses in systems and controls as manifested through SARs, and the use that should be made of such information. It will also identify clear processes and standards for deconflicting criminal and regulatory investigations.

3.19 The **NECC**, through the JMLIT, and the **Office for Professional Body Anti-Money Laundering Supervision (OPBAS)** will work with the **legal and accountancy professional body supervisors,** including through the **LSAG** and **AAG**, and law enforcement to facilitate and improve the appropriate and proportionate flow and use

of information and intelligence. This will include promoting the benefits of existing intelligence sharing arrangements, such as the FCA-facilitated Shared Intelligence Service and the Financial Intelligence Network, to further enhance the gathering and sharing of material on individuals and firms. OPBAS will also promote the appropriate and proportionate sharing of information between the professional body supervisors, particularly information relating to best practice, lessons learned and risk assessments and methodologies. OPBAS and the NECC have established JMLIT expert working groups for the legal and accountancy professional body supervisors to better share tactical and strategic intelligence with the NECC, law enforcement agencies and other statutory AML/CTF supervisors.

Action 10: Promote information-sharing in relation to fraud

3.20 Informed by the work of the information-sharing working group and to enhance information-sharing arrangements to prevent fraud**,** the **Home Office** will revise and update by December 2020:

- the list of Specified Anti-Fraud Organisations (SAFOs), with whom public authorities are allowed to share information in accordance with the *Serious Crime Act 2007;* and
- the statutory Code of Practice on data sharing with SAFOs, considering the latest ICO recommendations on information-sharing between public and private sectors for the purposes of preventing fraud.

3.21 The **Cabinet Office** will use the *Digital Economy Act 2017* to pilot data-sharing between organisations that could not previously occur to further understand fraud loss. Cabinet Office will complete the piloting of sharing known fraud data between the public and private sectors through the Counter Fraud Data Alliance and reach a decision with partners on whether to invest in an operational service by March 2020. Both sectors will work together to promote and build information and practice-sharing groups involving both sectors.

Strategic Priority Three: Powers, Procedures and Tools

Objective

Ensure the powers, procedures and tools of law enforcement, the justice system and the private sector are as effective as possible

Introduction

4.1 The FATF MER and UNCAC review both found that the UK has a strong legislative regime for combatting economic crime. We are committed to ensuring that these powers are used effectively and keep pace with evolving criminal threats and technological change.

4.2 The government has been proactive in putting this principle into effect. The incorporation of the EU's 4th Money Laundering Directive through the 2017 MLRs represented a wholesale update of the UK's AML/CTF regulatory regime to include the latest international standards. The *Criminal Finances Act 2017* enabled law enforcement to make better use of the intelligence in SARs and introduced powers to identify and recover criminal funds from those seeking to hide, use or move them in the UK. Powers introduced included Unexplained Wealth Orders, which can be used to compel individuals to explain the source of wealth used to purchase assets, and Account Freezing Orders to freeze and then forfeit illicit funds held in bank accounts. The NCA has frozen more than £160 million using the new tools.

Case study: SAR enables return of USD 500 million in alleged corrupt funds

In 2017, the UKFIU received a SAR from a reporter, regarding a USD 500 million transaction. On receipt of the SAR, the UKFIU analysed it and identified 'politically exposed person' links and so referred it to the NCA's International Corruption Unit for advice. Enquiries suggested the transaction appeared to be embezzlement and grand corruption, likely designed to steal the funds from a victim country. To ensure the monies were returned safely, the NCA needed to make enquiries of the victim country's authorities. Using the new SARs tools, the NCA was granted an extended period in which to conduct its enquiries. Following the receipt of several assurances safeguarding the account, the UKFIU granted consent that the USD 500 million could be returned to the victim country.

4.3 The Home Office, Scottish Government and Northern Ireland Executive all work with law enforcement agencies within their jurisdictions to develop and use powers set out in the *Proceeds of Crime Act 2002* (POCA). Alongside this plan, we are publishing an Asset Recovery Action Plan (ARAP) to set out the additional steps England and Wales will take to improve asset recovery performance.

4.4 In addition to our powers to recover criminal assets, it is essential the powers and tools of law enforcement and prosecutors, regulators and the private sector work effectively to combat economic crime. The Ministry of Justice issued a Call for Evidence on Corporate Criminal Liability in 2017 to examine whether there is a case for reform to ensure that the law in this area is fit for purpose.[37] The Call for Evidence set out five possible areas for reform including legislating to amend the current common law rules, consideration of a new form of vicarious liability; a new liability offence along the line of the existing failure to prevent model for Section 7 of the *Bribery Act 2010*, a variant of the failure to prevent model, and scope for further regulatory reform. The Ministry of Justice will be publishing the response to the Call for Evidence shortly.

4.5 We will also ensure that our AML/CTF preventive regime meets international best practice through the transposition of the EU's Fifth Money Laundering Directive and remains effective and responsive to the evolving threat environment. We will enable the criminal justice system to evolve with technological change. We will also ensure we have sufficient powers available to return funds to victims of fraud and supervise the private sector for implementation of their targeted financial sanctions obligations, review our criminal market abuse regime and investigate a power to block listings on national security grounds.

The public-private partnership

4.6 In developing these powers, we will work with the regulated and other sectors to ensure that such powers will operate effectively and impose as little burden as possible on legitimate businesses. We will consult on proposed new powers, procedures and tools as appropriate. As set out in the ARAP we will also work with the private sector to develop a public-private partnership approach to tackling those who seek to frustrate or evade the enforcement of confiscation orders.

Projects and Commitments

Action 11: Implement the Asset Recovery Action Plan

4.7 Law enforcement agencies in England and Wales, led by the **Home Office**, will implement the ARAP by July 2022.[38] The ARAP, which is published alongside this plan, sets out how we will ensure that:

- the legal framework is commensurate to the changing operational demands and available to the right operational agencies;
- improve our end-to-end operational systems, including to tackle the stock of uncollected orders, and determining the role the private sector should play;

[37] Ministry of Justice, Corporate Liability for Economic Crime: Call for Evidence, https://www.gov.uk/government/consultations/corporate-liability-for-economic-crime-call-for-evidence.

[38] Home Office, Asset Recovery Action Plan, https://www.gov.uk/crime-justice-and-law/crime-prevention.

- better understand what works to ensure our efforts are targeted and to inform future investment and operational decisions; and
- develop innovative new approaches to pursue and recover proceeds of crime, including the use of technology and partnership approaches to improve the identification and pursuit of criminal finances.

Action 12: Consider legislative changes to improve the Proceeds of Crime Act

4.8 Based on recommendations from the Law Commission's reviews of Parts 2 and 7 of POCA in England and Wales,[39] the **Home Office** will consider introducing legislative changes to POCA, where appropriate, to ensure law enforcement agencies have the most suitable powers. We anticipate that the Law Commission's review will be completed by early 2020 and, subject to Parliamentary time, proposals to amend POCA will be outlined by December 2021. We will ensure that the powers that are already enacted are available to all of those who need them and actively promote their use and will identify whether there are areas where extending powers to identify and seize suspected criminal property would be appropriate.

Action 13: Transpose the Fifth Money Laundering Directive

4.9 **HMT** will deliver the UK's expected obligation[40] to transpose the Fifth Money Laundering Directive (5MLD) into national law by January 2020. HMT are seeking to transpose in a way which balances the burden on business with the need for regulated businesses to actively deter money laundering and terrorist financing activity.[41] Key changes introduced by 5MLD include the incorporation of cryptoasset providers (see Action 37) and other entities as obliged entities under the MLRs, the expansion of the UK's trusts register and the introduction of a national register of bank account ownership.

Action 14: Implement the Disclosure Review recommendations

4.10 The emergence of digital technologies, which make available vast amounts of data, have posed challenges to the efficiency and effectiveness of disclosure in the criminal justice system, particularly in complex economic crime cases. The **Attorney General's Office** will lead the implementation of the recommendations made in the Attorney General's November 2018 Review of the Efficiency and Effectiveness of

[39] Further information is available on the Law Commission's website: https://www.lawcom.gov.uk/project/confiscation-under-part-2-of-the-proceeds-of-crime-act-2002/.

[40] In implementing 5MLD, the government is catering for the scenario where an implementation period is in place after the UK leaves the EU.

[41] HM Treasury, Transposition of the Fifth Money Laundering Directive, https://www.gov.uk/government/consultations/transposition-of-the-fifth-money-laundering-directive.

Disclosure in the criminal justice system by December 2019.[42] This, alongside work led by the **Crown Prosecution Service** and the **National Police Chiefs' Council** as part of the National Disclosure Improvement Plan, will ensure improvements in the performance of disclosure obligations in the criminal justice system.[43]

Action 15: Consider tactical targeting orders

4.11 To ensure we have the necessary powers for effective investigative action, the **Home Office, HM Treasury** and **UKFIU** will consider with reference to the SARs Transformation Programme (see Action 30), whether there is value in introducing a power similar to the geographical targeting orders used in the United States by July 2020.[44] This would assess whether such a power would assist with the collection of intelligence on particular crime threats in the UK context, subject to strict safeguards to ensure that the powers are used proportionately.

Action 16: Develop framework to repatriate funds to victims of fraud

4.12 The **Home Office**, working with the **JFT** and **UK Finance**, will develop the technical and legal framework to allow fraudulent funds to be taken from criminals and repatriated to victims by December 2021. This work will be informed by the broader projects to improve our support for victims of fraud (see Action 27) and review information-sharing arrangements (see Action 6) and take account of existing arrangements and requirements, such as the SARs regime, which enable law enforcement intervention into suspected fraudulent movement of funds.

Action 17: Clarify sanctions supervision powers

4.13 **HM Treasury**, with support of the **AML/CTF supervisors** including through the **LSAG** and **AAG**, will consider by July 2020 whether new powers or guidance are necessary to enable all supervisors to take enforcement action where there are deficiencies relating to financial sanctions regimes systems and controls in their regulated populations. The FATF MER recommended the UK review and formalise supervisors' powers to monitor sanctions systems and controls.

---

[42] Attorney-General's Office, Review of the Efficiency and Effectiveness of Disclosure in the Criminal Justice System, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/756436/Attorney_General_s_Disclosure_Review.pdf.

[43] National Police Chiefs' Council, College of Policing, Crown Prosecution Service, National Disclosure Improvement Plan, https://www.cps.gov.uk/sites/default/files/documents/publications/National-Disclosure-Improvement-Plan-May-2018.pdf.

[44] Further information is available on the US Department of the Treasury's Financial Crimes Enforcement Network's website: https://www.fincen.gov/sites/default/files/shared/Real%20Estate%20GTO%20FAQs_111518_FINAL%20508.pdf.

Action 18: Review the criminal market abuse regime

4.14 The criminal market abuse regime sets out the UK's criminal sanctions for insider dealing and market manipulation. It is important in helping the FCA fulfil its statutory objectives of protecting consumers, enhancing market integrity and promoting competition. The regime has not been materially updated since it was introduced. To ensure that the UK continues to effectively combat market abuse, it is prudent to review the current regime to consider any challenges to its objective.

4.15 Therefore, the **FCA** and **HM Treasury** will review the criminal market abuse regime by July 2021 and update it, where appropriate, to ensure that the UK's regime for combatting market abuse continues to work effectively in an evolving market.

Action 19: Investigate power to block listings on national security grounds

4.16 As recommended in the Treasury Select Committee's report, **HM Treasury** will lead on an investigation into whether a power to block listings on national security grounds would be appropriate. The first phase of this work will be concluded by June 2020. This investigation will evaluate the existing legislative framework, including analysis of the UK's post-Brexit sanctions powers under the *Sanctions and Anti-Money Laundering Act 2018*, as well as the impact a power could have on UK financial markets. If HM Treasury assesses that a new power is necessary, the government will clearly set out: a robust justification for the power, the scenarios in which it could be used, how the power would be implemented in practice, and the timing of the new legislation. The government would also undertake a full consultation on this power.

Strategic Priority Four: Enhanced Capabilities

Objective

Strengthen the capabilities of law enforcement, the justice system and private sector to detect, deter and disrupt economic crime

Introduction

5.1 To ensure that the UK is able to address our economic crime threats, the capabilities of the public and private sectors must remain robust and fit-for-purpose. The ever-changing and multi-faceted nature of the economic crime threat has made this a challenge. Innovative solutions are necessary to make use of the vast quantities of data and information now available to the public and private sectors. We need to have a better understanding of our current collective capabilities for combatting economic crime so that we can develop and deploy the right capabilities at the right time. We must ensure that the technologies that enable the transaction process are convenient enough for customers to use, agile enough to identify economic crime and robust enough to prevent it before it has taken place. We must make the environment as difficult as possible for criminals and fraudsters to operate while allowing business and society to prosper.

5.2 The UK has developed strong capabilities to tackle economic crime. Government is investing £48 million over 2019/20 in law enforcement's capabilities to combat economic crime by:

- continuing to build the NECC, which will reach out to public and private sector partners to increase capability and expand the expertise of its existing multi-agency resource;
- establishing the National Data Exploitation Capability (NDEC) in the NCA, which will harness analytics, automation, machine learning, bulk data ingestion and algorithms to improve our exploitation of data;
- expanding the NAC to provide a single authoritative view of the national serious and organised economic crime threat;
- building the capability and capacity at a local, regional and national level to tackle fraud and recognising fraud investigation as a specialist capability; and
- uplifting the NCA's investigative capabilities to detect and disrupt high-end economic crime cases, including a commitment to extend the NCA's directed tasking powers to include the Serious Fraud Office. Following consent from the Home Secretary and the Attorney General, this power will enable the

Director General of the NCA to task the Director of the SFO in relation to her investigatory functions.

5.3 The private sector in the UK invests heavily in preventing, detecting and investigating economic crime and protecting customers from fraud, through their compliance with regulatory obligations, training and awareness-raising. For the financial sector, this investment has generated 20 million financial crime alerts and related investigations per year, including 460,000 SARs flagging suspicious transactions in 2018/19. UK Finance estimates that technology, through measures such as biometric profiling and procedures to verify customers and devices, as well as artificial intelligence and machine learning, has stopped 67% of attempted frauds. Private sector organisations have also invested significant amounts in public-private efforts to combat economic crime, such as the Banking Protocol,[45] Mules Insights Tactical Initiative,[46] Don't Be Fooled campaign[47] and the Authorised Push Payment voluntary code,[48] to further enhance collaborative capabilities.

5.4 We need to build on these investments and embrace innovative technological solutions to make us collectively much more efficient and effective in combatting economic crime. Criminals continuously adapt and exploit new technologies and innovations. For example, while 'Confirmation of Payee' and stronger customer authentication under the revised Payment Services Directive will help reduce fraud, fraudsters will not stand still.[49] As some avenues for fraud are closed, they may look to exploit others.

5.5 The actions below set out a range of activity to better improve and coordinate our operational response to economic crime, leveraging the capabilities, skills and expertise of both public and private sectors. As recommended in the Treasury Select Committee's economic crime report, we will work together to identify opportunities to develop long-term, sustainable funding models to support this work and economic crime reform. This is a priority area of work as we recognise that the success of the plan is dependent upon ensuring that there is sufficient capacity across the public and private sectors to respond to the scale of the threat. This is not only about investing in additional infrastructure and capabilities, but also in ensuring that existing resources are used more effectively and efficiently. Action 38 sets out how we intend to promote innovative 'RegTech' solutions to enhance the private sector response to economic crime.

5.6 These actions also set out the next steps in our collective effort to reform the SARs regime and UKFIU. The SARs regime is a critical centrepoint in the UK's

---

[45] Further information is available on UK Finance's website: https://www.ukfinance.org.uk/news-and-insight/blogs/why-banking-protocol-matters.

[46] Mules Insights Tactical Initiative is a new anti-fraud measure, recently launched by Pay.UK in cooperation with UK Finance, using technology to track suspicious payments across different accounts and banks and help identify money mule accounts.

[47] UK Finance and Cifas are partnering on the Don't Be Fooled education and awareness campaign, which aims to inform students and young people about the risks of giving out their bank details, and deter them from becoming money mules.

[48] Further information is available on the Authorised Push Payments Scams Steering Group website: https://appcrmsteeringgroup.uk/.

[49] Further information is available on Confirmation of Payee is available on Pay.UK's website: https://www.wearepay.uk/confirmation-of-payee/.

system for combatting economic crime. As recognised in the FATF's 2018 MER, the SARs regime delivers significant outcomes against economic and wider crime, including terrorist financing and money laundering investigations and asset recovery results. Considering the scale of the threat faced by the UK, this system must be working as effectively as possible to produce the high quality financial intelligence necessary to detect and disrupt economic crimes. The FATF MER recommended that the UK reform the SARs regime and UKFIU as a priority. The NCA has increased the operational staffing in the UKFIU by over 30% with further appropriate increases to take place. The SARs Transformation Programme, led by the Home Office, aims to fundamentally reform the SARs operating model and deliver a regime with much better IT, enhanced feedback and a reformed UKFIU.

5.7 We also recognize that we need to continue to enhance the response of law enforcement and the criminal justice system to economic crime at the national and local level. A recent report by HMICFRS on the police response to fraud in England and Wales found that significant improvements are required to ensure it works more effectively and efficiently.[50] The Home Office will work closely with law enforcement to ensure an effective response to fraud at all levels. Joint public-private work to disrupt economic crime also offers a way to more effectively target our collective efforts. To ensure we have the appropriate criminal justice response to economic crime, we will also launch a flagship economic crime court.

5.8 It is critical that we ensure that we have the capability to close vulnerabilities that enable economic crimes to occur. The JFT is leading work to 'design out' vulnerabilities for fraud, which do not lie in the financial sector alone. Every business that maintains the records of customers online is vulnerable to data theft, and consequently can be an enabler of fraud. Hence cyber security must go hand-in-hand with any measures that are designed to reduce vulnerabilities. Transformative technologies like the New Payments Architecture must also be designed with economic crime concerns front-of-mind.

5.9 We will also ensure that we build resilience in the public sector, by continuing to build the Government's Counter Fraud Profession. The Profession aims to bring the counter fraud community together under a common set of standards and develop that community as they protect public services and fight economic crime.[51] We must also ensure we have the capability to support the victims of economic crime. Fraud is now the second most common crime in England and Wales and it is essential that victims of fraud are afforded the right level of care and we have the technological capabilities to identify where the proceeds of fraud have been transferred to and be able to repatriate those monies to victims (see Action 16).

The public-private partnership

5.10 The public and private sectors each have their own unique capabilities available to them to tackle economic crime, in terms of human, technical and

[50] Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services, Fraud: Time To Choose, https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf.

[51] Further information is available here: https://www.gov.uk/government/groups/counter-fraud-standards-and-profession.

financial resources. Historically, these capabilities have been viewed as separate, with insufficient consideration of how they can be combined and used collectively. We think there is substantial scope to enhance the public-private partnership around how our collective capabilities can be used. For example, the investigation of fraud is a specialist skill, and consequently lends itself to skill transfer or exchange between public and private sectors, where both sectors can learn from each other.

5.11 Steps have been taken in recent years to use the public and private sectors' capabilities together, through initiatives such as JMLIT, JFT and DCPCU. There is substantial scope to strengthen the public-private partnership through greater joint working and the collective use of capabilities. For example, the JFT was established in 2016 as a collaboration between the banking sector and government. It became apparent that tackling fraud required collaboration with other sectors beyond banking. That is why we have extended membership to retailers and the telecommunications sector, but we must not stop there. Many frauds, for example, originate or are facilitated through online platforms. We must draw on a broad range of industry expertise to tackle fraud that affects us all.

Projects & Commitments

Improving our collective capabilities

Action 20: Continue to develop the NECC as a genuine public-private hub for combatting serious and organised economic crime

5.12 By July 2021, the **NECC** will be fully established as the law enforcement lead for serious and organised economic crime in England and Wales, leading and coordinating and tasking across a whole system response to priority serious and organised crime threats such as high-end money laundering. It will include:

- working with the public and private sectors and law enforcement to embed people in the NECC;
- clear information protocols across NECC partners, including the private sector;
- supporting and directing partners on achieving operational performance and impact against the threat; and
- operating as the collective voice for serious and organised economic crime within law enforcement, identifying capability gaps, owning a single picture of the threat and driving the operational response.

Action 21: Understand and enhance capabilities

5.13 **NECC** will map the capabilities of law enforcement by July 2020 to develop a better understanding and enhance future capability. This will build on pre-existing work to map capabilities in the public sector. **Cabinet Office** will map the capabilities for combatting economic crime in central government.

5.14 **UK Finance** will also map the capabilities of the major financial institutions within its membership by July 2020. UK Finance will work with other relevant industry bodies to assist mapping of relevant institutions in their membership. The mapping

exercise will inform future work on taking system-wide action against major economic crime threats.

5.15 **NECC** will work with JMLIT sectors outside of banking to identify how best their skills, experience and capability can be harnessed to combat economic crime.

Action 22: Develop public-private action plans to combat economic crime threats

5.16 The NECC-led inaugural public-private serious and organised economic crime threat update identified a number of key economic crime threats (see Action 1). To truly tackle these threats, the full capabilities of the public and private sectors need to be harnessed. The **NECC, Home Office** and **HM Treasury** will ensure the findings of the first public-private threat update are reflected in activity in our operational and policy response. Where appropriate, **UK Finance** will coordinate the response on behalf of its membership and work with other industry associations to support this approach. Careful consideration should be given to which sectors should be involved in addressing a specific threat and to their respective capabilities and capacity.

5.17 This could include campaign-style responses to priority threats and weeks of action using collective capabilities of the public and private sectors. To facilitate this, the **NECC** will deliver threat-focused action plans summarising the proposed response to the identified threat, which could include threats such as money mules or the criminal exploitation of money service businesses. The first of these plans will be delivered to the next Economic Crime Strategic Board in January 2020.

Action 23: Develop a sustainable, long-term resourcing model for economic crime reform

5.18 **Home Office**, supported by **HM Treasury** and the **NCA**, will develop a long-term and sustainable resourcing model to support economic crime reform by March 2020. The development of this model will include consideration of resourcing for the SARs Transformation Programme, the UKFIU, Register of Bank Account Ownership and other key NCA capabilities such as the NECC.

5.19 The SARs Transformation Programme, is currently estimated to have costs of approximately £100-150 million and the target operating model end state is likely to see a significantly enhanced UKFIU which will require an ongoing sustainable resourcing model (see Action 30). Transforming the SARs regime will result in benefits for both the public and private sectors. Therefore the resourcing model will explore sources of funding from both sectors. A wide range of partners will be included in the funding solution, whilst keeping in mind the FATF standards on FIU independence and autonomy.

5.20 This work will also include the **Home Office** reviewing the Asset Recovery Incentivisation Scheme by March 2020 and the criteria for which funds are used, with particular consideration of whether the funds collected should be ring-fenced by the Home Office to be spent on economic crime projects.

5.21 With the support of **UK Finance** and other industry associations, this strategy should consider the more efficient and effective use of public and private resources in financial and economic crime investigations. This should consider the review of

financial investigator capability and capacity and the Proceeds of Crime Centre being conducted as part of the ARAP (see Action 11): the use of secondments; joint public-private work on financial intelligence and economic crime investigations; and joint training on economic crime issues.

5.22 With support from **Cabinet Office**, this should also consider the development of a structured exchange of experienced fraud investigators between public and private sectors as the Counter Fraud Profession develops (see Action 29).

Action 24: Launch flagship economic crime court in central London

5.23 **HM Courts and Tribunal Service (HMCTS),** an executive agency of the **Ministry of Justice**, is working with the **City of London Corporation** and the judiciary, to create a new world class economic crime court in Central London.

5.24 The flagship court will tackle fraud and related economic crime, including the expanding area of cybercrime, whilst also hearing other cases. It will hold 18 modern courtrooms and replace and upgrade the civil court, the Mayor's and City of London County Court, and City of London Magistrates' Court, and include eight Crown Court rooms. The site for the new court will be in the demolition stage by 2022, with an expectation that the court will be fully completed by 2026.

Action 25: Consider how payments systems can help tackle economic crime

5.25 The New Payments Architecture (NPA), a new interbank payment system, is currently in the design phase.[52] It is expected to go live after 2021, subject to detailed implementation and migration planning. **Pay.UK**, the payment system operator, is responsible for procuring the core clearing infrastructure for the NPA and for developing standards and rules to facilitate delivery of payment services. Pay.UK will consider how the design of the NPA could help tackle economic crime, with the support of **Payment Systems Regulator**, **FCA, HM Treasury** and **UK Finance** and other relevant agencies, including through:

- developing standards and rules to facilitate the introduction of new end-user services;[53]
- aligning, where appropriate, with the objectives and outcomes of other major capabilities being built (e.g. SARs Reform, Register of Bank Account Ownership, see Actions 13 and 30);[54] and
- adopting standards to allow for more comprehensive and flexible payments information.

[52] Further information is available on the Pay.UK website: https://www.wearepay.uk/new-payments-architecture-programme/.

[53] This includes Confirmation of Payee, which is already being delivered through the NPA programme. Further information is on Pay.UK's website: https://www.wearepay.uk/confirmation-of-payee/

[54] For example discussions are underway about providing payments data and setting standards and rules to facilitate the development of market-led transaction data analytics capabilities.

5.26 As part of the NPA programme Pay.UK is validating the Payment Strategy Forum's Blueprint for the NPA and considering a suitable role for Pay.UK on economic crime issues.[55] As part of consideration of its role and approach, Pay.UK also participates in relevant fraud and economic crime bodies.

5.27 The **Bank of England,** as operator for the Real-Time Gross Settlement system and Clearing House Automated Payment System (CHAPS), will also continue to consider how to tackle economic crime as appropriate given the nature of the services. For example, the Bank is working closely with Pay.UK on the development of interoperable message standards (such as the Common Credit Message)[56] and promoting wider adoption of Legal Entity Identifiers. This will enable, amongst other benefits, the introduction of enhanced payments data to be introduced in CHAPS and UK payment systems more widely.

Enhancing our response to fraud

Action 26: Improve the policing response to fraud

5.28 The **Home Office** will work with the **City of London Police** and the **NECC** to address the current deficiencies in the law enforcement response to fraud (including serious and organised fraud) in England and Wales, including those identified within HMICFRS's inspection report on the police response to fraud by March 2020. Our efforts will focus on:

- developing a clearer understanding of the threat to improve the targeting of resources;
- improving law enforcement's capabilities to help prevent, and protect people against, fraud;
- strengthening fraud reporting, referral, prioritisation and coordination processes;
- clarifying national, regional and local law enforcement responsibilities and how they should work together, including the role of the NECC;
- developing specialist fraud analysis and investigation capabilities, building partnerships with the wider public and private sectors, to improve law enforcement outcomes; and
- improving the provision of support to fraud victims.

5.29 The HMICFRS report also identifies the limited understanding of the serious and organised fraud threat caused by the low levels of investigation and the lack of organised crime group mapping. The **NECC** will:

[55] Further information is available on the Payments Strategy Forum's website: https://implementation.paymentsforum.uk/key-documents.

[56] Bank of England, ISO 20022 Consultation Paper: A Global Standard to Modernise UK Payments, https://www.bankofengland.co.uk/news/2018/june/iso-20022-consultation-paper-a-global-standard-to-modernise-uk-payments.

- conduct a review of the serious and organised fraud landscape and make recommendations to improve the understanding and response;
- together with the NDEC, undertake a data exploitation exercise to ingest and analyse a number of existing data sets to identify individuals and organised crime groups engaged in serious fraud;
- develop the use of tasking processes to ensure the most harmful cases are prioritised and receive appropriate support; and
- undertake analysis of the current systems for international intelligence exchange and provide recommendations to improve performance.

Action 27: Improve support for victims of fraud

5.30 The second objective of the 2018 SOC Strategy commits the government to building the highest levels of defence and resilience to protect vulnerable people, communities, businesses and systems. The recent HMICFRS report on the policing response to fraud also highlighted that whilst vulnerable victims generally receive a good service, most victims do not. The **Home Office**, alongside partners in law enforcement, National Trading Standards, wider government and the JFT, will consider an updated model for supporting victims of fraud, including enhanced capabilities locally, regionally and nationally, by August 2020.

5.31 This holistic review of support for victims of fraud will be informed by the existing Economic Crime Victims Care Unit model, through which specialist advocates provide support to those who have fallen victim to fraud and cyber-crime, and which aims to reduce the likelihood that they will become repeat victims.

Action 28: Close the vulnerabilities that criminals exploit to conduct fraud

5.32 The **JFT** will lead a programme of work to address the vulnerabilities that criminals exploit to conduct fraud by December 2020. The JFT will work with its diverse range of partners, including the telecommunications sector, to address vulnerabilities it identifies from its comprehensive understanding of the threat and identify potential legislative and regulatory solutions. The JFT will prioritise its efforts on the actions that will have the greatest impact on reducing the level of, and harm caused by, fraud.

Action 29: Build our Government Counter Fraud Profession

5.33 The **Cabinet Office** will continue to develop the Government Counter Fraud Profession, through on-boarding new members and developing the Profession to cover disciplines outside of investigation, including risk and threat assessment, and the use of data and analytics to find fraud by April 2021. The Cabinet Office will also explore the extension of the Profession to other sectors and review the powers

available to public sector investigators who are part of the Profession to ensure they are as effective as possible by April 2021.

SARs Reform and UKFIU

Action 30: Deliver first tranche of SARs IT transformation and design the target operating model for the future of the SARs regime

5.34 Working closely in collaboration with private sector stakeholders and law enforcement, the **SARs Transformation Programme** will agree the next iteration of the target operating model for the future SARs regime by December 2020. Alongside designing the future regime, the Transformation Programme is also defining and implementing shorter term improvements to the regime to improve effectiveness and efficiency. This includes the **NCA** delivering the first tranche of the IT transformation of the SARs regime, as well as delivery of some near-term improvements.

5.35 The future SARs regime will look to promote a 'whole system' approach to economic crime to deliver significantly higher levels of detection, prevention and enforcement (nationally and internationally).

5.36 Full delivery of the target operating model will look to transform the regime across people, processes and technology, delivering:

- more efficient and flexible IT portals and platforms for law enforcement and reporters to improve operational effectiveness, including an upgraded SAR submission process for reporters tailored to all different reporting sectors' needs, improved law enforcement tools to access and analyse SARs and a better system workflow to support UKFIU in managing SARs;
- improvements to regime processes and support to increase operational effectiveness of both reporters and law enforcement;
- a comprehensive regime-wide approach to feedback and guidance to iteratively improve SARs quality and regime processes (see Action 31);
- improved SARs analysis and intelligence through additional analytical resource and capabilities to the UKFIU and Regional Organised Crime Units; and
- training, outreach and awareness within law enforcement across the country to boost engagement and exploitation of SAR intelligence in the prevention, detection and investigation of all crimes.

5.37 This work will also address the FATF's criticisms regarding the role and resourcing of the UKFIU. Supported by the Programme, the **NCA** will ensure the UKFIU meets international best practice by December 2020. **Home Office**, supported by **HM Treasury** and **NCA,** will consider whether any legislative changes are necessary to meet the requirement under international standards for UKFIU to be sufficiently operationally independent and autonomous.

5.38 The Programme is also investigating the potential for further enhancements to the regime, including: increased availability of transaction-based data; clearer direction to the private sector on priorities for law enforcement through collaboration

with the NECC; and reviewing the 'Defence Against Money Laundering' SARs system. The Programme will also consider the findings of the Law Commission's review of POCA.[57] It is estimated that full delivery of the target operating model will take until 2023/24.

Action 31: Deliver greater feedback and engagement on SARs

5.39 Through the **SARs Transformation Programme**, the **UKFIU**, working with law enforcement and supervisory partners, will substantially enhance its capacity to deliver feedback to reporters on SARs reporting. Through improved IT and increased outreach capability, this will include greater information on trends in reporting and typologies, and will be informed by the work on information-sharing outlined in Action 6.

5.40 The transformed SARs IT will include a portal through which UKFIU will be able to communicate securely and directly with reporters. The portal will enable SARs to be reported and the UKFIU to share feedback and information on typologies, trends, economic crime alerts and outcomes on successful cases. The Programme will also provide increased financial intelligence analysts to undertake greater analysis of SARs and provide greater engagement with reporters, starting in 2020.

5.41 By December 2019, the **Home Office** will also identify the division of responsibility for the quality of SARs between UKFIU, supervisors, law enforcement and firms, which will help guide the better provision of feedback.

Action 32: Ensure the confidentiality of the SARs regime

5.42 SARs material is confidential and there is a need to protect the information in SARs and the source of the material. Arrangements are in place to guide the protection of this material from use in criminal proceedings.[58] However, there is a need to improve protection in parallel circumstances of civil proceedings. The **Home Office** and **UKFIU,** with the support of **HMT,** will work together to develop options to protect SARs material from being disclosed in civil proceedings.

[57] Law Commission, Anti-Money Laundering: The SARs Regime, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2019/06/6.5569_LC_Anti-Money-Laundering_Report_FINAL_WEB_120619.pdf.

[58] Home Office, Circular 022/2015, https://www.gov.uk/government/publications/circular-0222015-money-laundering-the-confidentiality-and-sensitivity-of-suspicious-activity-reports-sars-and-the-identity-of-those-who-make-them/circular-0222015-money-laundering-the-confidentiality-and-sensitivity-of-suspicious-activity-reports-sars-and-the-identity-of-those-who-make-them.

Strategic Priority Five: Risk-Based Supervision and Risk Management

Objective

Build greater resilience to economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision

Introduction

6.1 The preventive measures that businesses deploy to detect and prevent economic crime are the system's first line of defence. Through a strengthened private sector response, visible supervision and enforcement and greater individual resilience, we can better protect our society from economic crime. Building greater resilience to economic crime across the system makes it harder for criminals to penetrate in the first place. This in turn prevents the harm caused by economic crime, thereby reducing demand on law enforcement and other parts of the system.

6.2 A risk-based approach is central to the prevention of economic crime. When undertaken effectively, it enables firms and supervisors to focus their efforts and resources where the risks are highest, creating a robust regime at a proportionate cost. The vast majority of regulated firms want to comply with the law and take their responsibility to tackle economic crime seriously. Part of the role of the supervisors is to help them to do so through the provision of guidance and support. However, there is a minority who, either unwittingly or through wilful complicity, expose the UK to considerable risk and harm by facilitating or carrying out economic crime. In those circumstances, it is the role of the supervisors to take robust and decisive action, including through enforcement action where appropriate.

6.3 In the UK, firms have a range of regulatory obligations to help ensure they are not misused for economic crime purposes. The MLRs place AML/CTF preventive measures on a range of financial and non-financial sectors, such as gambling, legal, accountancy and property. Firms must also comply with financial sanctions and with anti-bribery obligations as well as protecting themselves and their customers from being defrauded. FCA authorised firms involved in certain markets must report suspected market abuse to the FCA.

6.4 The FATF MER found that implementation of the MLRs by the regulated sectors was inconsistent, with low levels of SAR reporting in several sectors, particularly the legal, accountancy and trust and company service provider sectors, highlighted as a concern. While noting positive steps to enhance supervision had been taken, the MER found significant weaknesses in the risk-based approach to supervision among all the UK's supervisors, except for the Gambling Commission. The MER also assessed the statutory supervisors and the Solicitors Regulation Authority as having a stronger understanding of the risks present in their sectors than the other professional body supervisors.

6.5 The actions below set out how we will increase our ability to prevent economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision, as well as building resilience in the wider community. As set out in Action 13, we will ensure that our preventive regime meets international best practice through the transposition of 5MLD.

6.6 We will ensure that our supervisors take an effective risk-based approach to supervision. The UK's position as a major global financial centre means we have a range of diverse sectors exposed to economic crime risks. It is essential for our security and prosperity that there are consistently high standards across all sectors. The FCA will review how it can have the greatest impact across the wide range of firms it supervises as well as continuing to apply proportionate, effective and dissuasive sanctions for AML/CTF breaches and enhancing its efforts to tackle market abuse. HMRC supervises a diverse range of high risk sectors and will make use of its recent increase in fees to develop a more comprehensive and robust risk-based strategy.

6.7 Stopping those professionals who, whether unwittingly or complicitly, enable criminals to enjoy the proceeds of their crimes, is vital in tackling economic crime at the root. The 22 legal and accountancy professional bodies AML/CTF supervisors have a clear duty to ensure that their members fully understand and adhere to proper standards of professional conduct in preventing and reporting money laundering. To facilitate collaboration and information-sharing and ensure the professional body supervisors meet the standards required by the MLRs, the government introduced OPBAS in January 2018. In March 2019, OPBAS published a summary of its first-year assessment of the professional body supervisors, finding varying quality of supervision.[59] OPBAS will work with the professional body supervisors to strengthen the consistency of their AML/CTF supervision.

6.8 We will also prioritise the development of innovative technological solutions to improve industry's preventive measures. We will promote the use of 'RegTech' solutions, such as digital identity and automated transaction monitoring services, to assist industry in becoming more efficient and effective in mitigating economic crime risks. This will include working with firms to ensure they strengthen their own defences, are resilient and take an appropriately holistic approach to their internal management of economic crime risks. For a true 'whole system' response, we will ensure that the broader public is better aware of the threats posed by economic crime through awareness-raising and education campaigns, so that all of society can take steps to protect itself from economic crime.

The public-private partnership

6.9 It is important to recognise that supervisors must remain independent in their ability to supervise. The actions committed to in this plan in no way limit that independence. Nonetheless, both the active supervision by supervisors and implementation of regulatory obligations by regulated firms are necessary for an effective response to economic crime. Through the implementation of this plan, the

[59] OPBAS and FCA, Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors, https://www.fca.org.uk/publication/opbas/themes-2018-opbas-anti-money-laundering-supervisory-assessments.pdf.

statutory and professional body supervisors should continue to deepen their partnership, ensuring that best practice is shared and that successful innovation in one part of the supervisory regime is replicated elsewhere. Supervisors will continue to assist firms in fulfilling their regulatory obligations in the most efficient and effective way, including through encouraging responsible innovation. Where necessary and appropriate, supervisors will take proportionate, effective and dissuasive action, including through civil and criminal enforcement actions.

Projects & Commitments

Risk-based supervision and the UK's regulatory regime

Action 33: Review the MLRs and OPBAS Regulations

6.10 **HMT** will lead a comprehensive review of the effectiveness and scope of the MLRs and the OPBAS Regulations and publish a report before 26 June 2022.[60] This will be an opportunity to measure the impact of the existing regulations, assess the proportionality of the duties and powers, the effectiveness of enforcement actions taken under the MLRs, the interaction of the MLRs with other pieces of legislation (like POCA) and consider options for reform. The review will be informed by analysis of impact as well as feedback from industry, law enforcement, supervisors and the broader public and civil society. The review will commence in 2021.

Action 34: Enhance FCA supervision and engagement

6.11 The **FCA** will continue to enhance its risk-based approach to AML/CTF supervision in response to the FATF MER. This will include consideration of how it can have the greatest impact across the range of firms it supervises through greater use of intelligence and data, including through the expanded use of the information collected in its annual data return. The FCA will have identified the changes it wants to make by March 2020 so they can commence implementation of changes in the next financial year (by March 2021).

6.12 The **FCA** will also continue regular engagement with industry associations to share supervisory findings from its AML/CTF programmes and engage with their members, supplemented by other AML/CTF-specific forums and events, which it intends to maintain and expand.

6.13 The **FCA** will, in partnership with the **Pensions Regulator**, continue its ScamSmart pension scams campaign. This will be supported with supervision and enforcement work to tackle scams and fraud more broadly. The FCA uses a range of data sources, including its 'Financial Lives' survey to gauge how prevalent these scams are as part of a broader effort to understand fraud risk.

6.14 The **FCA** will also continue to enhance its efforts to tackle market abuse. Over the next three years, the FCA will focus on:

[60] Under the MLRs, the government is required to undertake a review of the MLRs by this date.

- strengthening relationships with key partner organisations to improve intelligence gathering and investigations;
- educating market participants to improve standards of conduct, targeting the highest risk areas of the market;
- building the next generation in-house market surveillance capability so that the FCA can identify behaviours such as cross-market trading manipulation;
- enhancing specialist supervisory focus on the STOR regime in fixed income and commodities; and
- investigating suspicious activity, underpinned by strengthened proactive intelligence and more effective pursuit of the highest risk offenders.

Action 35: Enhance HMRC supervision

6.15 **HMRC** will deliver an enhanced risk-based approach to its AML/CTF supervision by March 2021, supported by the recent increase in charges to its supervised population. This will include tightened registration processes, greater use of behavioural science and educational material to increase compliance and an increase in interventions across their supervisory population which includes money service businesses, trust and company service providers, estate agents, high-value dealers and accountancy service providers. This will include a full review of HMRC's AML/CTF Supervision Operating model, recommendations to improve processes, and implementation of the new operating model and a new sanctions framework to ensure a robust approach that uses the full range of HMRC's powers effectively by April 2020.

6.16 HMRC will also carry out an annual self-assessment of its supervision's alignment to the **OPBAS** sourcebook standards. The first will begin in Autumn 2019 and the findings will be published in HMRC's 2020 supervision report. **HMT** will review and approve the self-assessment to ensure its comprehensiveness, consulting with OPBAS as part of this process. HMRC and OPBAS have formed a joint working group to strengthen HMRC's understanding of the OPBAS sourcebook and to support OPBAS' facilitation of collaboration and information-sharing between the professional body supervisors and statutory supervisors (see Action 9).

Action 36: Strengthen the consistency of professional body AML/CTF supervision

6.17 By December 2019, **OPBAS** will work with the **accountancy and legal professional body supervisors** to ensure they have appropriate AML/CTF strategy plans in place to address OPBAS' findings from its first report relating to their AML/CTF supervisory functions under the MLRs. OPBAS will monitor how these strategies are implemented, including formally contacting professional body supervisors on a regular basis to ensure they meet the deadlines and follow up with them to ensure they are suitably addressing ongoing actions. Following this, OPBAS will continue to monitor the professional body supervisors to deliver more consistent AML/CTF supervision by March 2021.

6.18 Following the Treasury Select Committee's recommendation, **HMT** will publish a detailed consideration of the process for responding to an OPBAS recommendation to remove a professional body supervisor's status as an AML/CTF supervisor, including managing changes in supervisory responsibilities, by September 2019.

Action 37: Establish the FCA as the supervisor of the future cryptoassets AML/CTF regime

6.19 The government is developing a robust regulatory response to address the risks posed by the use of cryptoassets for illicit activity, as identified by the FATF and the Cryptoasset Taskforce.[61] The government therefore plans to go beyond the requirements set out in 5MLD (see Action 13), bringing all relevant cryptoasset businesses into AML/CTF regulation in January 2020. This will aim to not only meet the latest international standards but provide one of the most comprehensive responses globally to the use of cryptoassets for illicit activity. The **FCA** will be the AML/CTF supervisor of cryptoasset firms, drawing on its considerable experience in this area. In recognising the risks that these types of activities pose, the government is considering expanding the FCA's supervisory toolkit to ensure it has the appropriate means by which to introduce and maintain a strong AML regime in the UK for relevant cryptoassets firms.

Industry implementation and risk-management

Action 38: Support innovation in regulatory compliance for AML/CTF

6.20 The **FCA** will continue to engage with the private sector to support innovation related to AML/CTF (i.e. RegTech). This will include continuing to encourage businesses with innovative solutions to engage with its Regulatory Sandbox,[62] running TechSprints, exploring new data-sharing technologies and considering how to provide clarity to firms on the use of innovative approaches to monitor customer relationships to detect money laundering and terrorist financing.

6.21 **HMT** and **UK Finance**, working with **FCA, Home Office,** the **Corporation of the City of London** and other public and private partners, will establish a new, senior-level Innovation Working Group to explore how to promote innovation and RegTech solutions to improve the effectiveness and efficiency of private sector preventive measures.

6.22 This group will consider what the barriers are to the adoption of innovative new solutions that could increase effectiveness and efficiency and agree solutions to addressing these barriers.

[61] HM Treasury, FCA, Bank of England, Cryptoassets Taskforce: Final Report, https://www.gov.uk/government/publications/cryptoassets-taskforce.

[62] Further information on the Regulatory Sandbox is available on the FCA's website: https://www.fca.org.uk/firms/regulatory-sandAction.

Action 39: Enhance firms' holistic response to economic crime

6.23 **UK Finance** and other **relevant industry associations** will work with its member firms to help the industry bolster their own defences and resilience and promote greater connectivity between their separate business units, such as their fraud, compliance and financial intelligence functions. This would enhance firms' counter-fraud efforts beyond risk management to make more consistent use of wider financial crime compliance systems. This should include the development and promotion of industry good practice, such as the Authorised Push Payment voluntary code, and promote information-sharing between different economic crime units with institutions to ensure organisations can engage holistically with law enforcement.

Action 40: Promote digital identity services

6.24 **HMT** will work with the new **Digital Identity Unit** and public and private partners to promote digital identity services. This will include working with FATF to produce new guidance clarifying the application of FATF's customer due diligence requirements to digital identity products and services by October 2019. It will also include changes to domestic guidance and/or regulations to reflect updates in 5MLD and to provide additional information on verification standards. In changing domestic guidance, HMT will work with the bodies responsible for producing AML/CTF guidance (**Joint Money Laundering Steering Group, HMRC, Gambling Commission, Legal Sector Affinity Group** and the **Consultative Committee of Accountancy Bodies**).

Building community resilience

Action 41: Education and awareness-raising on economic crime threats and the recovery of criminal assets

6.25 Informed by the understanding of the threat developed by the **NECC, UK Finance** and **Home Office**, together with other public and private partners including **LSAG** and **AAG**, will lead the development of an enhanced approach to education and awareness-raising of economic crime threats by December 2019. This work, which will be part of a broader strategic communications plan on economic crime, should identify what the priority economic crime threats are for targeting through education campaigns and whether additional research on how best to effect behavioural change in the target groups is necessary. Particular consideration will be given to deterring money mules.

6.26 This work should review and consider the lessons learned from the following major economic crime campaigns:

- the Flag It Up campaign, which is targeted at promoting SAR reporting by the accountancy, legal and property sectors;[63] and
- the Take Five campaign, which is targeted at helping customers protect themselves from preventable financial fraud.[64]

6.27 As set out in the ARAP, **Home Office** will also consider how best to empower communities and harness wider public engagement to help identify high end criminal assets and where they are located (see Action 11).

COMMISSION OF INQUIRY INTO STATE CAPTURE

[63] Further information is available here: https://flagitup.campaign.gov.uk/.

[64] Further information is available here: https://takefive-stopfraud.org.uk/.

Strategic Priority Six: Transparency of Ownership

Objective

Improve our systems for transparency of ownership of legal entities and legal arrangements

Introduction

7.1 Identifying who owns and ultimately controls a corporate entity is vital to expose wrongdoing and disrupt economic crime. The overwhelming proportion of the over 4 million UK companies are used for legitimate purposes. The misuse of legal entities in recent years however – through scandals including the Global and Azerbaijani Laundromats – has undermined the UK's reputation for clean business and demonstrated how criminals continue to use complex corporate structures to conceal their involvement in, and launder the proceeds of, their illegal activity. Improving the accuracy of information we hold on the ultimate ownership and control of UK registered legal entities and improving our understanding of the true beneficiaries of other legal arrangements such as trusts has been at the heart of the government's efforts to tackle the most pressing risks facing the UK.

7.2 The UK has been a global pioneer in developing and implementing an effective transparency of ownership regime. The UK's G8 Presidency in 2013 established trade, tax and transparency as priority themes, with the UK committing unilaterally to make its central registry of company beneficial ownership publicly accessible. The 2016 London Anti-Corruption Summit agreed new commitments on ownership transparency.

7.3 The UK has also encouraged action by its Overseas Territories and Crown Dependencies in line with evolving international norms. In 2017, the UK government entered an agreement with these jurisdictions to allow law enforcement access to company beneficial ownership information within 24 hours, or one hour if needed. A Statutory Review of these arrangements, published in June 2019, has shown that these arrangements are operating well.[65] In parallel, a UK-led international campaign is seeking to strengthen beneficial ownership transparency internationally.

7.4 To improve transparency, the UK introduced the first public register of people with significant control over companies, commonly termed beneficial owners, in 2016. This was accompanied by related measures such as the abolition of bearer shares in companies. In 2018, FATF recognised the UK as 'a global leader in promoting corporate transparency', with the UK becoming only the eighth country assessed by FATF at that point to be found to have a substantially effective framework for transparency over corporate entities. However, FATF recommended further improvements to the quality of information held at Companies House.

[65] Home Office, Statutory Review of the Exchange of Notes Arrangements, https://www.gov.uk/government/publications/statutory-review-of-the-exchange-of-notes-arrangements.

7.5 As set out in this plan, the government has embarked on a set of measures to improve the UK's regime for transparency of ownership in recent years. Newly announced proposals to reform Companies House will, if implemented in full, ensure that it is equipped with greater legal powers to query and seek corroboration on information submitted to it, amend and update errors on the register and work more closely with law enforcement and other partners to support investigations into those engaging in illicit activity. In the short term, the UK is continuing to enhance the quality of information held at Companies House by:

- continuing to invest in and develop technological solutions to improve automated checks on information received;
- closer cooperation between Companies House and UK law enforcement bodies, including making law enforcement aware of the breadth of information held on the register;
- closer cooperation between Companies House and the private sector; and
- transposing requirements within 5MLD, which will require firms within the AML/CTF-regulated sectors to directly inform Companies House of discrepancies between the beneficial ownership information that they have obtained through their customer due diligence measures, and information held at Companies House.

7.6 To improve the effectiveness of detecting incorrect and possibly suspicious information on who ultimately owns and controls corporate entities, it is necessary to be able to cross check the information received from companies against accurate and regular sources of information from both public and private sector organisations, and intermediaries that interact with corporate entities at various stages over their lifetime. This depends on robust systems and active participants to record timely, accurate and up-to-date information, not only on the ultimate beneficial owners of corporate entities, but potentially on basic corporate information too, and for this information to be readily accessible to law enforcement. While it may never be possible to reach 100% accuracy of basic and beneficial ownership information, we must aim to make the information available as accurate as possible.

7.7 To ensure a truly comprehensive transparency of ownership regime the following measures will be progressed over the lifetime of the plan:

- The Department for Business, Energy and Industrial Strategy (BEIS), announced, in May 2019, proposals for reform of Companies House which will, if implemented in full, constitute the most significant reforms of the UK's company registration framework in 175 years.[66] These proposals have been brought forward following the extensive evidence that a minority of UK companies are misused to facilitate economic crime.
- Announced in December 2018, final proposals for reform of limited partnerships which will be brought forward when Parliamentary time allows. These proposals will build upon reforms in 2017, which brought Scottish limited partnerships into the scope of the UK's public register of beneficial

[66] BEIS, Corporate Transparency and Register Reform, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/799662/Corporate_transparency_and_register_reform.pdf.

ownership. Since introduction, the numbers of newly formed Scottish limited partnerships have fallen by 80% year-on-year.

- Finalising legislation, via Parliamentary pre-legislative scrutiny, that will establish a public register of the beneficial owners of overseas entities that own UK property (the Registration of Overseas Entities Bill). This register will be the first of its type in the world and bring new levels of transparency to overseas ownership of the UK property market.
- Expansion of the Trust Registration Service by implementing 5MLD to bring within scope all UK trusts, regardless of whether they generate a UK tax consequence, as well as all non-EEA trusts which acquire real estate within the UK. Beneficial ownership information will be publicly accessible to those that demonstrate a 'legitimate interest' in access to data on this register.

7.8 Efforts in the UK are not enough. To end the criminal abuse of companies, the world needs efficient ways to share and access high-quality information about who owns and controls companies. The UK will work with like-minded partners to create a new global norm of accessible company beneficial ownership information that is linked across borders. In addition, work is already underway in the UK to encourage take-up of the Legal Entity Identifier, a unique global identification standard which will increase transparency around ownership structures across borders.[67]

The public-private partnership

7.9 While the legal reforms outlined above sit with the public sector, enhanced information on the ownership of UK entities will benefit both private and public sectors. The private sector has a crucial role in ensuring the accuracy of beneficial ownership information while at the same time providing confidence in the effectiveness of their CDD measures. These public sector reforms can be greatly enhanced by fully utilising private sector client knowledge, which can build on the information held by Companies House. The benefit to law enforcement agencies in gaining free, instant access to more accurate and comprehensive information regarding the ownership of corporate structures is clear.

Projects and commitments

Action 42: Reform Companies House

7.10 **BEIS** is currently consulting on proposals that, if implemented in full, will fundamentally reform **Companies House**, including by giving it powers to query information submitted to the UK's company register, and to seek additional evidence/information where appropriate. This work will be integrated into Companies House's existing change programme, including reforms to ensure that Companies House is properly equipped to deliver these expanded functions, and with the right capabilities to challenge inaccurate or misleading information that is submitted. Any necessary changes to the statutory framework or the fees charged by Companies House to deliver these reforms should be put in place during the lifetime of this plan.

[67] Further information is at: https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei.

7.11 As is set out in BEIS' consultation of May 2019, there are a range of options for how the UK can improve the quality of information on the Companies House register. Through BEIS' consultation process, HMG should identify which of these approaches – including the verification of identities of directors, beneficial owners, and company presenters – should ultimately be implemented. Following reform, Companies House will play a more active role in the UK's wider system for combatting economic crime. This will include enhanced mechanisms by which Companies House can share information with HMRC and other law enforcement authorities, including through comparing information held about accounts filed by UK corporates. The increased volume of information held by Companies House will facilitate more readily the identification of suspicious activity or trends/patterns that cause concern. Depending on new legal powers, Companies House could develop new partnership work with public sector, private sector and civil society partners to identify high risk typologies and abuse patterns on the register.

Action 43: Introduce a requirement to report discrepancies of beneficial ownership information

7.12 **HM Treasury** will legislate by January 2020 to require regulated firms within the AML/CTF-regulated sectors to report discrepancies between beneficial ownership information available at Companies House, and information which they obtain through their own compliance checks. This will enhance the accuracy of information at Companies House in the short-term. This will occur as part of the 5MLD transposition (see Action 13). Broader reforms to Companies House will consider how company formation agents can evidence that they have conducted satisfactory CDD on their customers.

Action 44: Enhance transparency of overseas ownership of UK property and reform limited partnerships

7.13 The government confirmed in January 2018 the timetable by which it would deliver the 2016 Anti-Corruption Summit commitment to establish a public register of beneficial owners of non-UK entities that own or buy UK property. A draft Bill was published in July 2018 and underwent pre-legislative scrutiny in the spring of 2019. **BEIS** intends to introduce this Bill to Parliament early in the next Parliamentary session when Parliamentary time allows, with the register to be operational with the support of **Companies House** in 2021.

7.14 The government committed in December 2018 to reform limited partnerships, including through ensuring that limited partnerships could only be registered through a MLR-regulated company formation agent that is either supervised in the UK or subject to equivalent supervision requirements overseas, by requiring limited partnerships to maintain an ongoing connection with the UK and by giving Companies House a power to strike off from the register dissolved or inactive limited partnerships. **BEIS** will bring forward legislation to give effect to these commitments when Parliamentary time allows.

Strategic Priority Seven: International Strategy

Objective

Deliver an ambitious international strategy to enhance security, prosperity and the UK's global influence

Introduction

8.1 We aim to develop an ambitious international strategy to enhance the global commitment and capacity to combat economic crime that will strengthen security, prosperity and the rules-based international system. This will be achieved through the delivery of three supporting objectives:

- maintaining and where necessary strengthening international standards, conventions and norms, and ensuring they are being effectively implemented;
- supporting sustainable development by strengthening resilience to economic crime and illicit finance; and
- protecting and promoting the UK's reputation.

8.2 Tackling international illicit financial flows is a top priority for the UK. It is critical in terms of reducing threats to the UK, protecting and promoting the UK's role as a financial centre, and reducing the destabilising impacts of illicit finance on the wider world, particularly developing countries. Success on this agenda will underpin our support for the rules-based international system. Closer bilateral and regional cooperation on tackling economic crime can help improve collective defences, increase enforcement outcomes such as the recovery of proceeds of crime across international boundaries (as referenced in the ARAP at Action 11). Strong public-private partnerships will help the private sector better understand and manage economic crime risks in high-risk jurisdictions and emerging markets, where there can be complex relationships and policy tensions to be managed.

8.3 Continued security cooperation with the EU will help ensure that UK standards do not simply displace economic crime to more vulnerable and smaller jurisdictions. As the UK leaves the EU, we will continue to work to reach a shared commitment to address the threats we face together through a new, robust and comprehensive partnership.

8.4 As a stable democracy, a major exporter and overseas investor and the world's largest centre for cross-border banking, the UK is an attractive destination for the proceeds of crime originating from overseas-based organised crime groups. A high proportion of these criminal proceeds are used to fund further criminal activity, fuelling the cycle of crime. These illicit financial flows harm our economy, as well as

the integrity and reputation of our financial system. Money held in the UK by those linked to organised crime and/or corruption also has the potential to represent a threat to the UK's national security.

8.5 Economic crime undermines development by distorting governance and economic outcomes, diverting resources, locking in power within elites, undermining the rule of law, and enhancing inequality. It has a disproportionately significant impact on the economy and functioning of the state in developing countries. Developing countries are also a key focus for the efforts of this plan because the weak institutions, 'deals-based' environments and selective or unequal application of the rule of law in some developing countries makes them ripe for the enablement of illicit financial flows. Sustainable development, which eradicates poverty and creates the foundations for global security and prosperity, requires the UK to build alliances that shape global rules, financial systems and capital flows, and improve the provision of global public goods.

International Illicit finance is a term commonly used to describe financial proceeds of crime that cross any international border. This can take a number of different forms, for example:

- where a crime is committed in one country and the financial proceeds of that crime flow into another country, possibly via multiple other jurisdictions, before being deposited potentially in the form of money in a bank account or potentially invested into physical assets such as property;
- where a crime is committed in the UK and the financial proceeds of the crime are transmitted overseas, potentially through multiple jurisdictions; and
- where a UK-based person or company is complicit in facilitating transmission of the proceeds of crime, even if the money never enters the UK.

8.6 The FATF MER found that the UK has a highly effective understanding of the threats it faces. As outlined in the preceding chapters in this plan however, there is more to be done to enhance the UK's domestic response to economic crime. The UK must progress the necessary domestic reforms in order to engage operationally and at a strategic level as a highly credible international partner in the fight against international illicit financial flows and economic crime.

8.7 There is a vast range of work being undertaken both domestically and internationally by the public, private and third sectors, including those set out in the UK Anti-Corruption Strategy. The actions here are an articulation of the priority actions that the public and private sectors can undertake to reduce the threat and occurrence of economic crime internationally. They set out how we intend to improve our understanding of international illicit finance, increase compliance with international standards and enhance overseas capabilities. We also set out how we will enhance our capacity to pursue overseas corruption and bribery and support companies to do business with integrity in developing countries.

The public-private partnership

8.8 The public and private sectors have mutually reinforcing roles in tackling international economic crime and cross-border illicit financial flows. Strong domestic implementation of international standards is essential both in reducing the overall illicit finance threat to the UK and other countries and in providing the credibility and best practice to encourage others to follow suit. Effective national implementation of new standards can help to address regulatory fragmentation and complexity, simplifying private sector compliance and releasing specialist resources to focus on investigating and tackling international criminal networks.

8.9 The implementation of international standards overseas, particularly in priority jurisdictions, is essential to tackle illicit finance and economic crime. Engagement to build political will and capability is led by the public sector at a political level, but is dramatically enhanced through the support of the private sector. The joint threat assessment process can support public-private engagement with priority jurisdictions, such as by understanding pivotal financial centres where international illicit financial flows can be most effectively countered or where international economic crime is being displaced to more vulnerable jurisdictions. Improved compliance with international standards supports the UK private sector to work abroad by minimising risk and providing new opportunities to undertake business with integrity.

Projects and Commitments

Action 45: Improve understanding of the nature and impact of the international threat

8.10 To effectively target and prioritise engagement to have the maximum impact, there needs to be a shared understanding of the international economic crime and illicit finance threat. Understanding the threat is one of the key priorities of this plan and a common understanding of the international threat will inform the development of domestic and international action to mitigate the threats, both to the UK and globally. To achieve this, we will undertake the following:

- the **NECC** will continue to work with its partners and grow its international team to maximise the understanding of the threat posed to the UK by jurisdictions of risk, including through the public-private threat assessment process (see Action 1);
- the **UKFIU** will further increase its engagement with the Egmont Group of FIUs and bilaterally with other FIUs, engaging in projects that undertake analysis of international money flows, to protect the UK and the global financial system; and
- the **Home Office, HM Treasury** and **DFID** will establish a single coordinated UK government response to international illicit finance, with a shared understanding of the problem delivered through targeted analysis

including the Serious and Organised Crime Joint Analysis, the UK's NRAs, and thematic assessments.

Action 46: Joint work on meeting international standards

8.11 The international system as a whole is only as strong as its weakest link, and vulnerabilities in one jurisdiction or region can have an impact on the integrity of the international system as a whole. Some countries have demonstrated a lack of will and/or capacity to implement global standards and rules including those set out by FATF, Egmont, the OECD Anti-Bribery Convention, UNCAC and the UN Convention on Transnational Organised Crime. The UK's engagement with multilateral standard-setting bodies can be bolstered through bilateral relationships with priority countries to increase commitment and capability.

8.12 Building the will and capability to comply with international standards can be best progressed in partnership. To achieve this, we will undertake the following:

- the public sector, led by **Home Office** and **HM Treasury,** will continue to work towards implementing the recommendations agreed in March 2017 as part of the OECD Working Group on Bribery Phase 4 Report on Implementing the OECD's Anti-Bribery Convention as well as the findings of the 2018 FATF MER and UNCAC review;
- **HM Treasury,** through the government's Prosperity Fund**,** will support the FATF global network through dedicated funding to FATF-Style Regional Bodies, support for the FATF secretariat to increase its engagement with the global network and provide training to members, as well as increasingly engaging with the MERs conducted by the FATF-Style Regional Bodies and sharing best practice;
- led by **HM Treasury** and **UK Finance,** the public and private sectors will jointly engage with priority jurisdictions, presenting a shared understanding and commitment to support increased compliance with international standards. This could include, for example, sharing best practice for complying with the FATF standards and preparing for a MER. This will be delivered through a range of mechanisms with support from the **Corporation of the City of London**, such as UK-hosted events for foreign businesses and governments, bilateral engagement in priority countries and industry-led events focused on sharing experiences and best practice;
- led by **HM Treasury, Home Office** and **DFID**, the public and private sectors will co-ordinate the provision of technical assistance to provide end-to-end support to increase understanding and capability in the public and private sectors in priority jurisdictions;
- the **Home Office** will deliver a global programme to share expertise and build capacity to facilitate public-private financial information-sharing partnerships using shared expertise; to support more effective implementation of UNCAC, **FCO**, with the United Nations Office on Drugs and Crime, will continue their regionally focused work with parties to

address priority areas for reform and provide technical assistance and training to developing countries;

- to support greater transparency and scrutiny in public procurement decisions, the **FCO** will continue to work with the **Government Digital Service's** Global Digital Marketplace Programme to build capability in developing countries on digital procurement systems, standards, processes and policies, delivery planning and assurance, and publishing open contracting data. This will empower the public, private and social enterprise sectors and civil society, to mitigate economic crime and corruption risks; and
- to support the development of more effective approaches to combatting economic crime, **HM Treasury**, **Home Office** and **DFID** will increase engagement with the private sector and civil society to ensure that their views are shared with international forums on priority issues such as cross-border information sharing, beneficial ownership transparency, international bribery standards and the use of innovative technologies.

Action 47: Enhance overseas capabilities

8.13 Supporting other countries to tackle economic crime and illicit finance, as well as sharing and developing best practice, requires the UK to have sufficiently skilled technical resource in high priority areas, for example use of financial intelligence, specialist supervision, data analytics and risk analysis. There can be a tension between domestic priorities and international outreach and engagement. But recognising that domestic and international action are mutually supporting, managing resources in line with this will help to facilitate a holistic approach to reducing illicit financial flows and economic crime. These specialist skills can be found in both the public and private sectors, with each having a valuable contribution.

8.14 To meet this aim, we will undertake the following:

- **DFID** will initiate the development of a new hybrid platform (the **International Centre of Excellence**) combining highly qualified public, private and academic expertise in understanding and addressing international illicit finance, with capacity to both support overseas efforts and to enhance cooperation with priority jurisdictions;
- through the **Home Office's, DFID's** and **FCO's** SOCNet[68] and the new **DFID** illicit finance network, we will establish new coordinated networks of policy expertise dedicated to tackling illicit finance in existing and emerging regional and global financial centres;

[68] SOCnet, a key deliverable of the 2018 Serious and Organised Crime Strategy, is a tri-departmental network of 18 policy officers, based overseas. It includes an 'Illicit Finance' network with experts sitting in global financial centres.

- **DFID** will scope the establishment of a new Global Financial Investigators Academy to train financial investigators;
- **FCA, HMRC** and the **Gambling Commission** will consider international engagement and assistance in their business planning to facilitate the sharing of best practice with overseas supervisory counterparts and **HM Treasury** and **OPBAS** will support the development of links between professional body supervisors to share understanding of risk, best practice and the UK's experience in regulating professionals under the MLRs;
- led by the **NECC**, UK law enforcement agencies will continue to embed staff in high priority jurisdictions to facilitate closer working relationships and joint responses to shared threats, including, where appropriate, with the private sector;
- the **UKFIU** will increase its capacity to cooperate internationally and continue to engage with its counterpart FIUs to share expertise and perspective, both bilaterally and multilaterally; and
- **Cabinet Office** will continue to work with partners in other countries to share leading practice in fighting fraud against the public sector through ongoing leadership of the International Public Sector Fraud Forum.

Action 48: Strengthen capability to investigate and prosecute bribery and corruption overseas

8.15 With **DFID's** support, the public sector will increase UK law enforcement agencies' capability to investigate and prosecute the laundering of corrupt money from developing countries through the UK and bribery in developing countries by UK companies or citizens. Since this UK Aid programme began in 2006, almost £800m of assets stolen from developing countries have been restrained, confiscated or returned, 30 companies and individuals have been convicted in the UK of money laundering, bribery and corruption offences; and the programme has facilitated developing countries to pursue and complete their own cases.

8.16 From 2020 to 2025, UK Aid will continue and increase funding to the International Corruption Unit at the **NCA** and the **CPS** so they can increase their staffing. This will enable more action in the UK to recover and return assets stolen from developing countries by corrupt individuals, and to pursue UK companies and nationals who engage in bribery and corruption in developing countries.

8.17 The **FCO** will continue to fund the International Anti-Corruption Co-ordination Centre (IACCC), which brings together specialist law enforcement officers from multiple jurisdictions into a single location to target grand corruption, working to trace and freeze and ultimately return stolen assets. In 2018 the IACCC provided vital intelligence support to progress nine grand corruption investigations, two senior officials were arrested as a direct result and the IACCC identified and disseminated intelligence relating to £51 million of worldwide suspicious assets.

Action 49: Promoting integrity in business internationally

8.18 The government wants to improve its offer to businesses seeking to succeed in emerging markets and fast-growing developing countries. As committed to in the 2017 Anti-Corruption Strategy, the Prime Minister announced the cross-government Business Integrity Initiative in 2018. The Initiative, led by **DFID**, provides practical guidance especially on issues such as bribery and human rights concerns to help businesses trade with and invest in new markets and includes:

- online guidance for exporters highlighting integrity risks to be aware of when doing business abroad and signposting to resources;
- the Business Integrity Consultancy Service, which provides up to 5 days of match-funded, tailored guidance from a consultant on topics including legal requirements for business, prevention and risk mitigation, collective action and human rights; and
- market and sector specific guidance for Kenya, Pakistan and Mexico, delivered through three country pilots to test how HMG can effectively provide business integrity support through UK missions (from March 2019 to March 2020).

8.19 This support helps firms enjoy sustainable commercial success and promote the UK as a trustworthy partner in line with the 'Global Britain' strategy. While the Initiative has seed funding from DFID's International Action against Corruption programme of £1.4 million (2017-21), it is jointly implemented with other UK government departments, especially the **Department for International Trade** and the **FCO.** It will be also supported by the **Corporation of the City of London**, via their work on the Sustainable Development Capital Initiative.

8.20 The **FCO** will continue to support OECD in enhancing the wide range of existing work across the organisation to strengthen business integrity. This includes helping countries better understand the multi-dimensional risks of corruption and illicit finance through greater knowledge sharing and to mitigate these risks by increasing co-operation, institutional partnerships and targeted engagement.

Governance and the public-private partnership

Current governance

9.1 The Economic Crime Strategic Board sits at the top of the economic crime governance. Jointly chaired by the Home Secretary and the Chancellor, the Board includes cross-sectoral government and private sector representation. The Board drives the public and private sector response to economic crime by setting shared strategic priorities for tackling economic crime and ensuring resources are aligned to deliver these priorities. The Board also holds the economic crime system to account for performance against the strategic priorities. The Board is ultimately the body that is accountable for the development and delivery of this plan. The Board also has oversight of matters in Scotland and Northern Ireland which are reserved to the UK government. Responsibility for non-reserved criminal justice matters in Scotland and Northern Ireland lies with the Scottish Government and Northern Ireland Department of Justice.

9.2 The Board is supported by the Economic Crime Delivery Board, Private Sector Steering Group and other working groups. The Economic Crime Delivery Board, jointly chaired by the Permanent Secretary of Home Office and the Second Permanent Secretary of HM Treasury, provides senior oversight and drives forward the various components of economic crime reform within the public sector. The joint Home Office, HM Treasury and UK Finance-chaired Private Sector Steering Group brings together senior representatives from across the private sector including the financial, property, accountancy and legal sectors. It focuses on developing shared strategic priorities with the private sector and has led the development of this plan.

9.3 The economic crime governance is relatively new, with the current governance being formally established in June 2018. The new governance structure provides senior oversight of economic crime and is genuinely public-private for the first time. It is important that the governance continues to evolve to ensure that it effectively implements the actions outlined in this plan and addresses new threats as they emerge.

Projects and Commitments

Action 50: Review the economic crime governance

9.4 **Home Office** and **HM Treasury** will review the current economic crime governance by September 2019 to ensure it is able to effectively implement the actions set out in this plan. The review should consider whether there is appropriate representation from public and private sectors, noting the tension between inclusion and efficiency, and ensure there is sufficient accountability and transparency regarding the activity of the public-private economic crime governance.

9.5 The review will consider the links between the current economic crime governance and other governance structures and, where possible, seek rationalisation or better coordination across the following:

- serious and organised crime, cyber, terrorist financing and anti-corruption governance;
- the SARs Transformation Programme; and
- the NECC.

Action 51: Develop stronger public-private and private-private partnerships

9.6 **Home Office**, **HM Treasury** and **NECC** will lead outreach to better engage with sectors and organisations not currently represented in economic crime governance. This should consider the need to engage smaller and geographically-diverse organisations to ensure the full range of economic crime is being addressed and should also prioritise engagement with non-MLR regulated sectors such as social media, telecommunications and technology companies.

9.7 Informed by lessons learnt from platforms such as the JMLIT and Joint Money Laundering Steering Group,[69] **UK Finance** will work with other financial and payment associations, **LSAG, AAG** and the **Corporation of the City of London** to consider how best to enhance cross-sectoral cooperation in combatting economic crime. This could include the use of new or pre-existing governance and mechanisms to share information on best practice, lessons learned and ways of working, as well as identifying clear channels for cross-sectoral industry communication.

Action 52: Enhance engagement with civil society

9.8 Currently, the economic crime governance does not have any formal links with representatives from non-government organisations, academia, victims' groups and civil society. As part of the review of economic crime governance, **Home Office**, **HM Treasury** and **NECC** will work with civil society to create a formalised civil society-led mechanism to facilitate engagement on both our policy and operational response to economic crime.

[69] JMLSG is a private sector organisation that brings together trade bodies in the financial services sector to develop common guidance, as well as sector specific guidance, for meeting legislative and regulatory AML/CTF requirements.

Monitoring the plan

Review and accountability of the plan

10.1 The implementation of this plan will be overseen by the ministerial Economic Crime Strategic Board, which commissioned the development of this plan. The Board will review progress in implementing the plan and will test whether the actions are driving up the UK's response to economic crime. The Board will carry out a formal review of implementation of the plan and will make a statement on progress in July 2020.

10.2 The Economic Crime Delivery Board, Private Sector Steering Group and other relevant working groups will monitor implementation and coordinate progress on a more routine basis.

10.3 The plan is designed to be receptive to any major changes to the UK's economic crime threat profile. The Economic Crime Strategic Board may seek to update the priorities and actions in the plan to address the emergence of a new major economic crime threat.

Measuring success

10.4 This plan will be monitored against a set of key economic crime performance questions (KPQs), set out below, supplemented by the detailed evaluation of the impact of specific programmes. This will form part of the wider National Serious and Organised Crime Performance Framework, developed by the Home Office and NCA in conjunction with stakeholders from across the system, to deliver a quantitative and qualitative approach to understanding the impact of the UK's overseas and domestic response to serious and organised crime. This framework is overseen by the National Security Implementation Group on Serious and Organised Crime:

- KPQ 1: How comprehensive is our understanding of economic crime threats and vulnerabilities?
- KPQ 2: How effectively are we pursuing serious and organised economic criminals in the UK, online and overseas?
- KPQ 3: How effectively are we building resilience in the public and private sector against economic crime?
- KPQ 4: How effectively are we supporting those impacted by economic crime?
- KPQ 5: How effectively are we deterring people from involvement in economic crime?
- KPQ 6: How effectively are we developing core capabilities to address emerging economic crime threats?

- KPQ 7: How effectively and efficiently are we managing our resources in countering economic crime?

10.5 In addition, a performance framework will be developed to monitor progress towards the economic crime strategic objectives which introduce each chapter of this plan, and to make informed decisions about the most effective, efficient way to allocate and achieve value for money.

10.6 The UK's AML/CTF regime will also undergo a targeted review in 2023 as part of its fifth-year follow-up by the FATF following the 2018 MER. This will act as a focused re-evaluation of areas of weakness in the UK's AML/CTF regime.

COMMISSION OF INQUIRY INTO STATE CAPTURE

Annex A – Organisations consulted in development of this plan

This plan was developed through targeted consultation with the public and private sectors and civil society in the first half of 2019. In addition to the extensive consultation with public sector representatives, the following private sector and civil society organisations were consulted in the development of this economic crime plan through industry associations.

Accountancy

Accountancy Affinity Group
Association of Accounting Technicians
Association of Chartered Certified Accountants
Association of International Certified Professional Accountants
BDO
Bishop Fleming
Chartered Accountants Ireland
Chartered Institute of Taxation
Deloitte LLP
Ernst & Young LLP
Institute of Chartered Accountants England & Wales
Institute of Chartered Accountants Scotland
Institute of Financial Accountants
International Association of Bookkeepers
Mazars
KPMG
PWC
RSM
UHY

Banking, finance and payments

Answer Digital
Association of British Insurers
Association of Foreign Banks
Aviva
Aviva Investors
Barclays
Coinbase
Contis
Cornercard
DVB Bank
Electronic Money Association
Entersekt
Electronic Payments Association
Esure
Fintrail
First Abu Dhabi Bank PJSC
GBG
Go Cardless
Google
HSBC
Insurance and Life Assurance Group
Investment Association
Joint Money Laundering Steering Group
JP Morgan
Kompli
Lloyds Banking Group
Loot
LV
M&G
ModulrFinance
Morgan Stanley
National Bank of Greece
Nationwide
Optal

Paddle
Paybase
Paysafe Group
RBS
Refinitiv
Santander UK
Sarasin
Standard Chartered
SWIFT Institute
Tide
Transferwise
Trustly
Turkish Bank
UK Finance and UK Finance members involved in relevant panels
Verafin
Western Union
WorldFirst
W2 Global
Zurich

Gaming
British Amusement Catering Trade Association
British Racecourse Bookmakers' Association
Camelot
Federation of Racecourse Bookmakers Association
Hospice Lotteries Associations
Lotteries Council
National Casino Forum
Remote Gambling Association

Fraud
Cifas
Insurance Fraud Bureau

Legal
Aros Smith
Bar of Northern Ireland
Blackadders
Bordies
Bryan Cave Leighton Paisner
BTO
Clyde & Co
Dalling & Co
Faculty of Advocates
Harper Macleod
Herbert Smith Freehills
Hickman and Rose
Law Society of England and Wales
Law Society of Northern Ireland
Law Society of Scotland
Legal Sector Affinity Group
Mayer Brown
Peterkins
Solicitors Regulation Authority
Thorntons
Wright, Jonhston & Mackenzie

NGOs and academic
Cardiff University
Corruption Watch
Global Witness
Northumbria University
OSF
Police Foundation
Queen Mary University
Royal United Services Institute
Sheffield University
Tackling Economic Crime Awards
Tax Justice Network
University of West London

Property
Arnolds Key
Bedfords
Connells Group
Foxtons
National Association of Estate Agents
Quality Homes
Sawdye & Harris
Watsons Property

Annex B – Glossary

Meanings of key agencies, terms and acronyms

5MLD: Fifth Money Laundering Directive.

Accountancy Affinity Group (AAG): The AAG is a meeting of all of UK accountancy professional body AML/CTF supervisors which aims to support the achievement of the UK's AML/CTF regime through the development of guidance, sharing best practices, input to national developments and liaison with government.

Action Fraud: The UK's single point of reporting for fraud and cyber-crime.

AML/CTF: Anti-Money Laundering and Counter-Terrorist Financing.

AML/CTF supervisors: Supervisors oversee AML/CTF compliance for regulated entities. There are three statutory supervisors (FCA, HMRC and the Gambling Commission) and there are 22 approved professional body supervisors for supervising the legal and accountancy sectors.

Attorney General's Office (AGO): The AGO supports the Attorney General and the Solicitor General in their duty to provide legal advice to the UK government and to oversee the main prosecution authorities in England and Wales – the CPS and SFO.

Cabinet Office: The Cabinet Office supports the work of the National Security Council through the National Security Secretariat. The Cabinet Office is also the centre of the Government Counter Fraud Function, which brings together those working on fraud and economic crime across central government to set standards, develop capability and give expert advice. The Cabinet Office oversees the development of capability to counter fraud in the public sector, through the Government Counter Fraud Profession.

Companies House: Companies House is the registrar for UK legal persons.

Crown Prosecution Service (CPS): The CPS prosecutes serious and organised crime cases in England and Wales. CPS pursues all confiscation proceedings flowing from criminal investigations conducted by NCA and HMRC and undertakes both criminal confiscation and civil recovery proceedings in conjunction with ROCUs and police forces.

DCPCU: Dedicated Card and Payment Crime Unit.

Department for Business, Energy and Industrial Strategy (BEIS): BEIS is responsible for policy relating to business, including ensuring there is transparency around who ultimately owns and controls a company, which is an important part of the global fight against corruption, money laundering and terrorist financing.

Department for Digital, Culture, Media and Sport (DCMS): DCMS leads the government's relations with the technology industry, including with communications service providers, while also overseeing data protection responsibilities.

Department for International Development (DFID): DFID leads the UK's work to end extreme poverty and to deliver programmes to tackle insecurity and conflict in

developing countries. This includes addressing underlying social and economic problems (such as corruption) that enable serious and organised crime to flourish.

Devolved Administrations (DAs): DAs are responsible in Northern Ireland, Scotland and Wales for the functions which have been devolved to them according to their different devolution settlements. Policing and justice are devolved in Scotland, where they are overseen by the Justice and Safer Communities Directorates and to Northern Ireland where they are overseen by the Department of Justice. The Lord Advocate is responsible for the investigation and prosecution of crime in Scotland. The Economic Crime and Financial Investigation Unit of Police Scotland investigates economic crime in Scotland, and cases are then prosecuted by the Crown Office and Procurator Fiscal Service (COPFS), or in the case of civil recovery actions, they are pursued by the Civil Recovery Unit. The Economic Crime Unit of the Police Service of Northern Ireland (PSNI) leads financial crime investigations that are not the responsibility of a specialised agency (e.g. NCA or SFO), which are then prosecuted by the Public Prosecution Service of Northern Ireland.

FATF: Financial Action Task Force.

Financial Conduct Authority (FCA): The FCA regulates the financial sector and financial advisers, and will pursue criminal prosecutions, including for market manipulation. It is also an AML/CTF supervisor for financial institutions.

FIU: Financial Intelligence Unit.

Foreign and Commonwealth Office (FCO): The FCO is responsible for delivering diplomatic and practical support to our priorities overseas, including on AML/CTF, serious and organised crime and corruption.

HM Inspectorate of Constabulary, Fire Rescue Services (HMICFRS): HMICFRS independently assesses the effectiveness and efficiency of police forces and fire & rescue services. It assesses whether services are sufficient to meet the public interest and has a role to play in tackling corruption.

HM Revenue and Customs (HMRC): HMRC is the UK's tax and customs authority, responsible for tackling fiscal fraud, with civil and criminal powers to investigate tax fraud. It is also an AML/CTF supervisor, including of money service, estate agency, trust and company service and accountancy businesses and high value dealers.

HM Treasury (HMT): HMT is responsible for regulating the financial and banking sectors, for the MLRs and overseeing AML/CTF supervision. HMT leads the UK's engagement with the FATF.

Home Office: The Home Office is responsible for leading the UK's response to crime, working closely with the police, security and intelligence agencies and across government to do this. The Home Secretary and Minister of State for Security and Economic Crime have ministerial oversight at a policy level for the criminal justice aspects of the AML/CFT system, including national security and counter-terrorism policy, as well as oversight of the NCA.

Information Commissioner's Office (ICO): The ICO is the UK's independent body set up to uphold information rights.

Joint Fraud Taskforce (JFT): The JFT was set up in 2016, together with the private sector, law enforcement and government to protect the public from fraud.

Joint Money Laundering Intelligence Taskforce (JMLIT): Established in 2014 and launched as an operational pilot in 2015, the JMLIT has provided a mechanism for law enforcement and the financial sector to share information and work more closely together to detect, prevent and disrupt money laundering and wider economic crime. it is situated in the NECC.

Legal Sector Affinity Group (LSAG): The LSAG is a meeting of all of UK legal professional body AML/CTF supervisors which aims to support the achievement of the UK's AML/CTF regime through the development of guidance, sharing best of best practices, input to national developments and liaison with government.

MER: Mutual Evaluation Report.

MLRs: *Money Laundering, Terrorist Financing and Transfer of Funds Information on the Payer) Regulations 2017*

Ministry of Justice (MoJ): MoJ works to protect the public and reduce reoffending, and to provide a more effective, transparent and responsive criminal justice system for victims and the public. It is also responsible for ensuring that prison and probation services disrupt crime-related activity as part of a lifetime offender management approach.

NAC: National Assessments Centre.

National Crime Agency (NCA): The NCA leads and coordinates law enforcement's response to serious and organised crime in England and Wales and is responsible for developing a single authoritative view of the threat. The NCA also has a network of international liaison officers and is responsible for a number of national functions, including responsibility for liaising with Europol and Interpol. The NCA is led by a Director General and overseen by the Home Secretary, but is operationally independent.

National Economic Crime Centre (NECC): The NECC is a collaborative, multi-agency centre that has been established to deliver a step change in the response to tackling serious and organised economic crime. The NECC sets threat priorities which informs operational coordination between partners and facilitates the exchange of data and intelligence between the public and private sectors.

National Fraud Intelligence Bureau (NFIB): The NFIB is a unit in the City of London Police, responsible for gathering and analysing intelligence relating to fraud and financially-motivated cyber-crime.

National Police Chiefs' Council (NPCC): The NPCC is the body responsible for the coordination of policing operations, reform, driving improvements and ensuring value for money.

NDEC: National Data Exploitation Capability.

NPA: New Payments Architecture.

NRA: National Risk Assessment.

OECD: Organisation for Economic Co-operation and Development.

Office for Professional Body AML Supervision (OPBAS): OPBAS is an oversight body for the legal and accountancy sectors. It was created to address the weaknesses in AML/CTF supervision in the legal and accounting sectors identified in the 2015 NRA. It has a focus on improving application of the risk-based approach and ensuring that effective, proportionate and dissuasive sanctions are applied.

Office of Financial Sanctions Implementation (OFSI): A part of HM Treasury that helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom.

POCA: *Proceeds of Crime Act 2002*.

Police Forces: Most of the operational work against crime in the UK is conducted by the 43 police forces in England and Wales at a regional and local level and by the Police Service of Scotland (Police Scotland) and Police Service Northern Ireland (PSNI). The Metropolitan Police Service and the City of London Police in particular have dedicated teams in place to combat terrorism, money laundering, fraud and other economic crimes and also provide an operational arm for other law enforcement agencies. Officers of the Police Service of Scotland are subject to the direction of the Lord Advocate and the Procurator Fiscal.

Regional Organised Crime Units (ROCUs): ROCUs are regional police units that have a number of specialist capabilities used to investigate and disrupt serious and organised crime. There are nine ROCUs in England and in Wales and they are the principal interface between the NCA and police forces.

Regulated firms: Private sector firms with obligations under the MLRs.

SAFO: Specified Anti-Fraud Organisations.

SAR(s): Suspicious Activity Report(s).

Serious Fraud Office (SFO): The SFO is a specialist law enforcement agency that investigates and prosecutes the top level of serious and complex fraud, bribery and corruption, and associated money laundering.

STOR: Suspicious transaction and order reporting.

UNCAC: United Nations Convention Against Corruption.

UK Financial Intelligence Unit (UKFIU): The UKFIU is housed within the NCA and is responsible for receiving and disseminating SARs and conducting analysis in line with its statutory mandate.

Australia 2014

G20 High-Level Principles on Beneficial Ownership Transparency

The G20 considers financial transparency, in particular the transparency of beneficial ownership of legal persons and arrangements, is a high priority. The G20 Leaders' Declaration from St Petersburg states, 'We encourage all countries to tackle the risks raised by the opacity of legal persons and legal arrangements'. In order to maintain the momentum, Leaders called upon Finance Ministers to update them by the 2014 G20 Leaders' Summit on the steps taken by G20 countries 'to meet FATF standards regarding the beneficial ownership of companies and other legal arrangements such as trusts by G20 countries leading by example.'

At their meeting in Sydney in 2014, Finance Ministers and Central Bank Governors requested the ACWG provide them with an update before their April meeting on concrete actions the G20 could take to lead by example on beneficial ownership transparency and the implementation of relevant FATF standards. Following the G20 ACWG meeting in Sydney, ACWG co-chairs reported to Finance Ministers and Central Bank Governors that the ACWG agreed that G20 countries will lead by example by developing G20 High-Level Principles on Beneficial Ownership Transparency that will set out concrete measures G20 countries will take to prevent the misuse of and ensure transparency of legal persons and legal arrangements.

Improving the transparency of legal persons and arrangements is important to protect the integrity and transparency of the global financial system. Preventing the misuse of these entities for illicit purposes such as corruption, tax evasion and money laundering supports the G20 objectives of increasing growth through private sector investment.

The G20 is committed to leading by example by endorsing a set of core principles on the transparency of beneficial ownership of legal persons and arrangements that are applicable across G20 work streams. These principles build on existing international instruments and standards, and allow sufficient flexibility to for our different constitutional and legal frameworks.

1. Countries should have a definition of 'beneficial owner' that captures the natural person(s) who ultimately owns or controls the legal person or legal arrangement.

2. Countries should assess the existing and emerging risks associated with different types of legal persons and arrangements, which should be addressed from a domestic and international perspective.
    a. Appropriate information on the results of the risk assessments should be shared with competent authorities, financial institutions and designated non-financial businesses and professions (DNFBPs[1]) and, as appropriate, other jurisdictions.

[1] As identified by the Financial Action Task-force

b. Effective and proportionate measures should be taken to mitigate the risks identified.
c. Countries should identify high-risk sectors, and enhanced due diligence could be appropriately considered for such sectors.

3. Countries should ensure that legal persons maintain beneficial ownership information onshore and that information is adequate, accurate, and current.

4. Countries should ensure that competent authorities (including law enforcement and prosecutorial authorities, supervisory authorities, tax authorities and financial intelligence units) have timely access to adequate, accurate and current information regarding the beneficial ownership of legal persons. Countries could implement this, for example, through central registries of beneficial ownership of legal persons or other appropriate mechanisms.

5. Countries should ensure that trustees of express trusts maintain adequate, accurate and current beneficial ownership information, including information of settlors, the protector (if any) trustees and beneficiaries. These measures should also apply to other legal arrangements with a structure or function similar to express trusts.

6. Countries should ensure that competent authorities (including law enforcement and prosecutorial authorities, supervisory authorities, tax authorities and financial intelligence units) have timely access to adequate, accurate and current information regarding the beneficial ownership of legal arrangements.

7. Countries should require financial institutions and DNFBPs, including trust and company service providers, to identify and take reasonable measures, including taking into account country risks, to verify the beneficial ownership of their customers.
   a. Countries should consider facilitating access to beneficial ownership information by financial institutions and DNFBPs.
   b. Countries should ensure effective supervision of these obligations, including the establishment and enforcement of effective, proportionate and dissuasive sanctions for non-compliance.

8. Countries should ensure that their national authorities cooperate effectively domestically and internationally. Countries should also ensure that their competent authorities participate in information exchange on beneficial ownership with international counterparts in a timely and effective manner.

9. Countries should support G20 efforts to combat tax evasion by ensuring that beneficial ownership information is accessible to their tax authorities and can be exchanged with relevant international counterparts in a timely and effective manner.

10. Countries should address the misuse of legal persons and legal arrangements which may obstruct transparency, including:
    a. prohibiting the ongoing use of bearer shares and the creation of new bearer shares, or taking other effective measures to ensure that bearer shares and bearer share warrants are not misused; and
    b. taking effective measures to ensure that legal persons which allow nominee shareholders or nominee directors are not misused.

The G20 is committed to leading by example in implementing these agreed principles. As a next step, each G20 country commits to take concrete action and to share in writing steps to be taken to implement these principles and improve the effectiveness of our legal, regulatory and institutional frameworks with respect to beneficial ownership transparency.

COMMISSION OF INQUIRY INTO STATE CAPTURE

Financial Intelligence Centre Amendment Act, Act 1 of 2017

(South African Legislation)

COMMISSION OF INQUIRY INTO STATE CAPTURE

FATF

PH-269

INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION

The FATF Recommendations

COMMISSION OF INQUIRY INTO STATE CAPTURE

Updated June 2019

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website: www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2012-2019), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France, www.fatf-gafi.org/recommendations.html

© 2012-2019 FATF/OECD. All rights reserved.
No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING
OF TERRORISM & PROLIFERATION

THE FATF RECOMMENDATIONS

ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012

Updated June 2019

COMMISSION OF INQUIRY INTO STATE CAPTURE

CONTENTS

List of the FATF Recommendations 4

Introduction 6

FATF Recommendations 9

Interpretive Notes 29

Note on the legal basis of requirements on financial institutions and DNFBPs 108

Glossary 110

Table of Acronyms 125

Annex I: FATF Guidance Documents 126

Annex II: Information on updates made to the FATF Recommendations 127

© 2012-2019

THE FATF RECOMMENDATIONS

Number	Old Number[1]	
		A – AML/CFT POLICIES AND COORDINATION
1	-	Assessing risks & applying a risk-based approach *
2	R.31	National cooperation and coordination
		B – MONEY LAUNDERING AND CONFISCATION
3	R.1 & R.2	Money laundering offence *
4	R.3	Confiscation and provisional measures *
		C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	SRII	Terrorist financing offence *
6	SRIII	Targeted financial sanctions related to terrorism & terrorist financing *
7		Targeted financial sanctions related to proliferation *
8	SRVIII	Non-profit organisations *
		D – PREVENTIVE MEASURES
9	R.4	Financial institution secrecy laws
		Customer due diligence and record keeping
10	R.5	Customer due diligence *
11	R.10	Record keeping
		Additional measures for specific customers and activities
12	R.6	Politically exposed persons *
13	R.7	Correspondent banking *
14	SRVI	Money or value transfer services *
15	R.8	New technologies
16	SRVII	Wire transfers *
		Reliance, Controls and Financial Groups
17	R.9	Reliance on third parties *
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries *
19	R.21	Higher-risk countries *
		Reporting of suspicious transactions
20	R.13 & SRIV	Reporting of suspicious transactions *
21	R.14	Tipping-off and confidentiality
		Designated non-financial Businesses and Professions (DNFBPs)
22	R.12	DNFBPs: Customer due diligence *
23	R.16	DNFBPs: Other measures *

© 2012-2019

		E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
24	R.33	Transparency and beneficial ownership of legal persons *
25	R.34	Transparency and beneficial ownership of legal arrangements *
		F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
		Regulation and Supervision
26	R.23	Regulation and supervision of financial institutions *
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs
		Operational and Law Enforcement
29	R.26	Financial intelligence units *
30	R.27	Responsibilities of law enforcement and investigative authorities *
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers *
		General Requirements
33	R.32	Statistics
34	R.25	Guidance and feedback
		Sanctions
35	R.17	Sanctions
		G – INTERNATIONAL COOPERATION
36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation *
39	R.39	Extradition
40	R.40	Other forms of international cooperation *

1. *The 'old number' column refers to the corresponding 2003 FATF Recommendation.*

* *Recommendations marked with an asterisk have interpretive notes, which should be read in conjunction with the Recommendation.*

Version as adopted on 15 February 2012.

INTRODUCTION

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:

- identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;
- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- facilitate international cooperation.

The original FATF Forty Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In October 2001 the FATF expanded its mandate to deal with the issue of the funding of terrorist acts and terrorist organisations, and took the important step of creating the Eight (later expanded to Nine) Special Recommendations on Terrorist Financing. The FATF Recommendations were revised a second time in 2003, and these, together with the Special Recommendations, have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

© 2012-2019

Following the conclusion of the third round of mutual evaluations of its members, the FATF has reviewed and updated the FATF Recommendations, in close co-operation with the FATF-Style Regional Bodies (FSRBs) and the observer organisations, including the International Monetary Fund, the World Bank and the United Nations. The revisions address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations.

The FATF Standards have also been revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced. Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk. The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.

Combating terrorist financing is a very significant challenge. An effective AML/CFT system, in general, is important for addressing terrorist financing, and most measures previously focused on terrorist financing are now integrated throughout the Recommendations, therefore obviating the need for the Special Recommendations. However, there are some Recommendations that are unique to terrorist financing, which are set out in Section C of the FATF Recommendations. These are: Recommendation 5 (the criminalisation of terrorist financing); Recommendation 6 (targeted financial sanctions related to terrorism & terrorist financing); and Recommendation 8 (measures to prevent the misuse of non-profit organisations). The proliferation of weapons of mass destruction is also a significant security concern, and in 2008 the FATF's mandate was expanded to include dealing with the financing of proliferation of weapons of mass destruction. To combat this threat, the FATF has adopted a new Recommendation (Recommendation 7) aimed at ensuring consistent and effective implementation of targeted financial sanctions when these are called for by the UN Security Council.

The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary. The measures set out in the FATF Standards should be implemented by all members of the FATF and the FSRBs, and their implementation is assessed rigorously through Mutual Evaluation processes, and through the assessment processes of the International Monetary Fund and the World Bank – on the basis of the FATF's common assessment methodology. Some Interpretive Notes and definitions in the glossary include examples which illustrate how the requirements could be applied. These examples are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

The FATF also produces Guidance, Best Practice Papers, and other advice to assist countries with the implementation of the FATF standards. These other documents are not mandatory for assessing compliance with the Standards, but countries may find it valuable to have regard to them when considering how best to implement the FATF Standards. A list of current FATF Guidance and Best

Practice Papers, which are available on the FATF website, is included as an annex to the Recommendations.

The FATF is committed to maintaining a close and constructive dialogue with the private sector, civil society and other interested parties, as important partners in ensuring the integrity of the financial system. The revision of the Recommendations has involved extensive consultation, and has benefited from comments and suggestions from these stakeholders. Going forward and in accordance with its mandate, the FATF will continue to consider changes to the standards, as appropriate, in light of new information regarding emerging threats and vulnerabilities to the global financial system.

The FATF calls upon all countries to implement effective measures to bring their national systems for combating money laundering, terrorist financing and the financing of proliferation into compliance with the revised FATF Recommendations.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

THE FATF RECOMMENDATIONS

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach *

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation).

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence *

Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures *

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudicing the rights of *bona fide* third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations, or (d) property of corresponding value.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries should consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction (non-conviction based confiscation), or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

© 2012-2019

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence *

Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing *

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation *

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organisations *

Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including:

(a) by terrorist organisations posing as legitimate entities;

(b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and

(c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence *

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

© 2012-2019

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA) in accordance with the Interpretive Notes to this Recommendation and to Recommendation 1.

Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d) above (subject to appropriate modification of the extent of the measures on a risk-based approach), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons *

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

(b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and source of funds; and

(d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking *

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships;

(d) clearly understand the respective responsibilities of each institution; and

(e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

© 2012-2019

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. Money or value transfer services *

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes.

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

16. Wire transfers *

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing.

RELIANCE, CONTROLS AND FINANCIAL GROUPS

17. Reliance on third parties *

Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.

18. Internal controls and foreign branches and subsidiaries *

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-

© 2012-2019

wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

19. Higher-risk countries *

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

REPORTING OF SUSPICIOUS TRANSACTIONS

20. Reporting of suspicious transactions *

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. These provisions are not intended to inhibit information sharing under Recommendation 18.

DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. DNFBPs: customer due diligence *

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

(a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

(b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

(e) Trust and company service providers – when they prepare for or carry out transactions for a client concerning the following activities:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

23. DNFBPs: Other measures *

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d)

© 2012-2019

of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

(b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

COMMISSION OF INQUIRY INTO STATE CAPTURE

E. TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24. Transparency and beneficial ownership of legal persons *

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

25. Transparency and beneficial ownership of legal arrangements *

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

© 2012-2019

F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions *

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes, and which are also relevant to money laundering and terrorist financing, should apply in a similar manner for AML/CFT purposes. This should include applying consolidated group supervision for AML/CFT purposes.

Other financial institutions should be licensed or registered and adequately regulated, and subject to supervision or monitoring for AML/CFT purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution's license, where applicable.

28. Regulation and supervision of DNFBPs *

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum:

- casinos should be licensed;

- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, holding a management function in, or being an operator of, a casino; and
- competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements. This should be performed on a risk-sensitive basis. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a "fit and proper" test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.

OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units *

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities *

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialised in financial or asset investigations. Countries should ensure that, when necessary,

© 2012-2019

cooperative investigations with appropriate competent authorities in other countries take place.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

32. Cash couriers *

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4, which would enable the confiscation of such currency or instruments.

GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

© 2012-2019

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation. In particular, countries should:

(a) Not prohibit, or place unreasonable or unduly restrictive conditions on, the provision of mutual legal assistance.

(b) Ensure that they have clear and efficient processes for the timely prioritisation and execution of mutual legal assistance requests. Countries should use a central authority, or another established official mechanism, for effective transmission and execution of requests. To monitor progress on requests, a case management system should be maintained.

(c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

(d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions or DNFBPs to maintain secrecy or confidentiality (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).

(e) Maintain the confidentiality of mutual legal assistance requests they receive and the information contained in them, subject to fundamental principles of domestic law, in order to protect the integrity of the investigation or inquiry. If the requested country cannot comply with the requirement of confidentiality, it should promptly inform the requesting country.

Countries should render mutual legal assistance, notwithstanding the absence of dual criminality, if the assistance does not involve coercive actions. Countries should consider adopting such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Countries should ensure that, of the powers and investigative techniques required under Recommendation 31, and any other powers and investigative techniques available to their competent authorities:

(a) all those relating to the production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other persons, and the taking of witness statements; and

(b) a broad range of other powers and investigative techniques;

are also available for use in response to requests for mutual legal assistance, and, if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Countries should, when making mutual legal assistance requests, make best efforts to provide complete factual and legal information that will allow for timely and efficient execution of requests, including any need for urgency, and should send requests using expeditious means. Countries should, before sending requests, make best efforts to ascertain the legal requirements and formalities to obtain assistance.

The authorities responsible for mutual legal assistance (e.g. a Central Authority) should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

38. Mutual legal assistance: freezing and confiscation *

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value. This authority should include being able to respond to requests made on the basis of non-conviction-based confiscation proceedings and related provisional measures, unless this is inconsistent with fundamental principles of their domestic law. Countries should also have effective mechanisms for managing such property, instrumentalities or property of corresponding value, and arrangements for coordinating seizure and confiscation proceedings, which should include the sharing of confiscated assets.

© 2012-2019

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations. In particular, countries should:

(a) ensure money laundering and terrorist financing are extraditable offences;

(b) ensure that they have clear and efficient processes for the timely execution of extradition requests including prioritisation where appropriate. To monitor progress of requests a case management system should be maintained;

(c) not place unreasonable or unduly restrictive conditions on the execution of requests; and

(d) ensure they have an adequate legal framework for extradition.

Each country should either extradite its own nationals, or, where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case, without undue delay, to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Where dual criminality is required for extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Consistent with fundamental principles of domestic law, countries should have simplified extradition mechanisms, such as allowing direct transmission of requests for provisional arrests between appropriate authorities, extraditing persons based only on warrants of arrests or judgments, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings. The authorities responsible for extradition should be provided with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of such authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

40. Other forms of international cooperation *

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing

cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTES TO THE FATF RECOMMENDATIONS

INTERPRETIVE NOTE TO RECOMMENDATION 1 (ASSESSING RISKS AND APPLYING A RISK-BASED APPROACH)

1. The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

2. In implementing a RBA, financial institutions and DNFBPs should have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks. The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing. Specific Recommendations set out more precisely how this general principle applies to particular requirements. Countries may also, in strictly limited circumstances and where there is a proven low risk of money laundering and terrorist financing, decide not to apply certain Recommendations to a particular type of financial institution or activity, or DNFBP (see below). Equally, if countries determine through their risk assessments that there are types of institutions, activities, businesses or professions that are at risk of abuse from money laundering and terrorist financing, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors.

A. Obligations and decisions for countries

3. **Assessing risk** - Countries[1] should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

4. **Higher risk** - Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks, and, without prejudice to any other measures taken by countries to mitigate these higher risks, either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. Where the FATF Recommendations identify higher risk activities for which enhanced or specific measures are required, all such measures must be applied, although the extent of such measures may vary according to the specific level of risk.

5. **Lower risk** - Countries may decide to allow simplified measures for some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided that a lower risk has been identified, and this is consistent with the country's assessment of its money laundering and terrorist financing risks, as referred to in paragraph 3.

   Independent of any decision to specify certain lower risk categories in line with the previous paragraph, countries may also allow financial institutions and DNFBPs to apply simplified customer due diligence (CDD) measures, provided that the requirements set out in section B below ("Obligations and decisions for financial institutions and DNFBPs"), and in paragraph 7 below, are met.

6. **Exemptions** - Countries may decide not to apply some of the FATF Recommendations requiring financial institutions or DNFBPs to take certain actions, provided:

   (a) there is a proven low risk of money laundering and terrorist financing; this occurs in strictly limited and justified circumstances; and it relates to a particular type of financial institution or activity, or DNFBP; or

   (b) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing.

---

[1] Where appropriate, AML/CFT risk assessments at a supra-national level should be taken into account when considering whether this obligation is satisfied.

© 2012-2019

While the information gathered may vary according to the level of risk, the requirements of Recommendation 11 to retain information should apply to whatever information is gathered.

7. **Supervision and monitoring of risk** - Supervisors (or SRBs for relevant DNFBPs sectors) should ensure that financial institutions and DNFBPs are effectively implementing the obligations set out below. When carrying out this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration.

B. Obligations and decisions for financial institutions and DNFBPs

8. **Assessing risk** - Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs. The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business. Financial institutions and DNFBPs should always understand their money laundering and terrorist financing risks, but competent authorities or SRBs may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

9. **Risk management and mitigation** - Financial institutions and DNFBPs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified (either by the country or by the financial institution or DNFBP). They should be required to monitor the implementation of those controls and to enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with national requirements and with guidance from competent authorities and SRBs.

10. **Higher risk** - Where higher risks are identified financial institutions and DNFBPs should be required to take enhanced measures to manage and mitigate the risks.

11. **Lower risk** - Where lower risks are identified, countries may allow financial institutions and DNFBPs to take simplified measures to manage and mitigate those risks.

12. When assessing risk, financial institutions and DNFBPs should consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level of mitigation to be applied. Financial institutions and DNFBPs may differentiate the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

INTERPRETIVE NOTE TO RECOMMENDATION 3 (MONEY LAUNDERING OFFENCE)

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

2. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches.

3. Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment.

4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

5. Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically.

6. Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

7. Countries should ensure that:

   (a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances.

   (b) Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of money laundering.

   (c) Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of

© 2012-2019

liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

(d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATIONS 4 AND 38 (CONFISCATION AND PROVISIONAL MEASURES)

Countries should establish mechanisms that will enable their competent authorities to effectively manage and, when necessary, dispose of, property that is frozen or seized, or has been confiscated. These mechanisms should be applicable both in the context of domestic proceedings, and pursuant to requests by foreign countries.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 5 (TERRORIST FINANCING OFFENCE)

A. Objectives

1. Recommendation 5 was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and, *inter alia*, money laundering, another objective of Recommendation 5 is to emphasise this link by obligating countries to include terrorist financing offences as predicate offences for money laundering.

B. Characteristics of the terrorist financing offence

2. Terrorist financing offences should extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.

3. Terrorist financing includes financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

4. Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy is not sufficient to comply with this Recommendation.

5. Terrorist financing offences should extend to any funds or other assets, whether from a legitimate or illegitimate source.

6. Terrorist financing offences should not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

7. Countries should ensure that the intent and knowledge required to prove the offence of terrorist financing may be inferred from objective factual circumstances.

8. Effective, proportionate and dissuasive criminal sanctions should apply to natural persons convicted of terrorist financing.

9. Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate and dissuasive.

10. It should also be an offence to attempt to commit the offence of terrorist financing.

11. It should also be an offence to engage in any of the following types of conduct:

    (a) Participating as an accomplice in an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(b) Organising or directing others to commit an offence, as set forth in paragraphs 2 or 9 of this Interpretive Note;

(c) Contributing to the commission of one or more offence(s), as set forth in paragraphs 2 or 9 of this Interpretive Note, by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

12. Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 6 (TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM AND TERRORIST FINANCING)

A. OBJECTIVE

1. Recommendation 6 requires each country to implement targeted financial sanctions to comply with the United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person[2] or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by Security Council resolution 1267 (1999) and its successor resolutions[3]; or (ii) any person or entity designated by that country pursuant to Security Council resolution 1373 (2001).

2. It should be stressed that none of the obligations in Recommendation 6 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by Recommendation 4 (confiscation and provisional measures)[4]. Measures under Recommendation 6 may complement criminal proceedings against a designated person or entity, and be adopted by a competent authority or a court, but are not conditional upon the existence of such proceedings. Instead, the focus of Recommendation 6 is on the preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups. In determining the limits of, or fostering widespread support for, an effective counter-terrorist financing regime, countries must also respect human rights, respect the rule of law, and recognise the rights of innocent third parties.

---

[2] Natural or legal person.

[3] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999) and any future UNSCRs which impose targeted financial sanctions in the terrorist financing context. At the time of issuance of this Interpretive Note, (February 2012), the successor resolutions to resolution 1267 (1999) are resolutions: 1333 (2000), 1363 (2001), 1390 (2002), 1452 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

[4] Based on requirements set, for instance, in the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)(the Vienna Convention)* and the *United Nations Convention against Transnational Organised Crime (2000) (the Palermo Convention),* which contain obligations regarding freezing, seizure and confiscation in the context of combating transnational crime. Additionally, the *International Convention for the Suppression of the Financing of Terrorism (1999)(the Terrorist Financing Convention)* contains obligations regarding freezing, seizure and confiscation in the context of combating terrorist financing. Those obligations exist separately and apart from the obligations set forth in Recommendation 6 and the United Nations Security Council Resolutions related to terrorist financing.

B. IDENTIFYING AND DESIGNATING PERSONS AND ENTITIES FINANCING OR SUPPORTING TERRORIST ACTIVITIES

3. For resolution 1267 (1999) and its successor resolutions, designations relating to Al-Qaida are made by the 1267 Committee, and designations pertaining to the Taliban and related threats to Afghanistan are made by the 1988 Committee, with both Committees acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), designations are made, at the national or supranational level, by a country or countries acting on their own motion, or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

4. Countries need to have the authority, and effective procedures or mechanisms, to identify and initiate proposals for designations of persons and entities targeted by resolution 1267 (1999) and its successor resolutions, consistent with the obligations set out in those Security Council resolutions[5]. Such authority and procedures or mechanisms are essential to propose persons and entities to the Security Council for designation in accordance with Security Council list-based programmes, pursuant to those Security Council resolutions. Countries also need to have the authority and effective procedures or mechanisms to identify and initiate designations of persons and entities pursuant to S/RES/1373 (2001), consistent with the obligations set out in that Security Council resolution. Such authority and procedures or mechanisms are essential to identify persons and entities who meet the criteria identified in resolution 1373 (2001), described in Section E. A country's regime to implement resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001), should include the following necessary elements:

   (a) Countries should identify a competent authority or a court as having responsibility for:

      (i) proposing to the 1267 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1989 (2011) (on Al-Qaida) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria;

      (ii) proposing to the 1988 Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation, as set forth in Security Council resolution 1988 (2011) (on the Taliban and those associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan) and related resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria; and

[5] The relevant Security Council resolutions do not require countries to identify persons or entities and submit these to the relevant United Nations Committees, but to have the authority and effective procedures and mechanisms in place to be able to do so.

© 2012-2019

(iii) designating persons or entities that meet the specific criteria for designation, as set forth in resolution 1373 (2001), as put forward either on the country's own motion or, after examining and giving effect to, if appropriate, the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

(b) Countries should have a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolution 1988 (2011) and resolution 1989 (2011) and related resolutions, and resolution 1373 (2001) (see Section E for the specific designation criteria of relevant Security Council resolutions). This includes having authority and effective procedures or mechanisms to examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries pursuant to resolution 1373 (2001). To ensure that effective cooperation is developed among countries, countries should ensure that, when receiving a request, they make a prompt determination whether they are satisfied, according to applicable (supra-) national principles, that the request is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2011), as set forth in Section E.

(c) The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) When deciding whether or not to make a (proposal for) designation, countries should apply an evidentiary standard of proof of "reasonable grounds" or "reasonable basis". For designations under resolutions 1373 (2001), the competent authority of each country will apply the legal standard of its own legal system regarding the kind and quantum of evidence for the determination that "reasonable grounds" or "reasonable basis" exist for a decision to designate a person or entity, and thus initiate an action under a freezing mechanism. This is the case irrespective of whether the proposed designation is being put forward on the relevant country's own motion or at the request of another country. Such (proposals for) designations should not be conditional upon the existence of a criminal proceeding.

(e) When proposing names to the 1267 Committee for inclusion on the Al-Qaida Sanctions List, pursuant to resolution 1267 (1999) and its successor resolutions, countries should:

(i) follow the procedures and standard forms for listing, as adopted by the 1267 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice;

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1267 Committee; and

(iv) specify whether their status as a designating state may be made known.

(f) When proposing names to the 1988 Committee for inclusion on the Taliban Sanctions List, pursuant to resolution 1988 (2011) and its successor resolutions, countries should:

(i) follow the procedures for listing, as adopted by the 1988 Committee;

(ii) provide as much relevant information as possible on the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of individuals, groups, undertakings, and entities, and to the extent possible, the information required by Interpol to issue a Special Notice; and

(iii) provide a statement of case which contains as much detail as possible on the basis for the listing, including: specific information supporting a determination that the person or entity meets the relevant designation (see Section E for the specific designation criteria of relevant Security Council resolutions); the nature of the information; supporting information or documents that can be provided; and details of any connection between the proposed designee and any currently designated person or entity. This statement of case should be releasable, upon request, except for the parts a Member State identifies as being confidential to the 1988 Committee.

(g) When requesting another country to give effect to the actions initiated under the freezing mechanisms that have been implemented pursuant to resolution 1373 (2001), the initiating country should provide as much detail as possible on: the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

© 2012-2019

(h) Countries should have procedures to be able to operate ex parte against a person or entity who has been identified and whose (proposal for) designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated by the 1267 Committee and 1988 Committee (in the case of resolution 1267 (1999) and its successor resolutions), when these Committees are acting under the authority of Chapter VII of the Charter of the United Nations. For resolution 1373 (2001), the obligation for countries to take freezing action and prohibit the dealing in funds or other assets of designated persons and entities, without delay, is triggered by a designation at the (supra-)national level, as put forward either on the country's own motion or at the request of another country, if the country receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee meets the criteria for designation in resolution 1373 (2001), as set forth in Section E.

6. Countries should establish the necessary legal authority and identify domestic competent authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

(a) Countries[6] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

(b) Countries should prohibit their nationals, or any persons and entities within their jurisdiction, from making any funds or other assets, economic resources, or financial or other related services, available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or

[6] In the case of the European Union (EU), which is a supra-national jurisdiction under Recommendation 6, the EU law applies as follows. The assets of designated persons and entities are frozen by the EU regulations and their amendments. EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

(c) Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

(d) Countries should require financial institutions and DNFBPs[7] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by the competent authorities.

(e) Countries should adopt effective measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 6.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of persons and entities designated pursuant to resolution 1267(1999) and its successor resolutions that, in the view of the country, do not or no longer meet the criteria for designation. In the event that the 1267 Committee or 1988 Committee has de-listed a person or entity, the obligation to freeze no longer exists. In the case of de-listing requests related to Al-Qaida, such procedures and criteria should be in accordance with procedures adopted by the 1267 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), and any successor resolutions. In the case of de-listing requests related to the Taliban and related threats to the peace, security and stability of Afghanistan, such procedures and criteria should be in accordance with procedures adopted by the 1988 Committee under Security Council resolutions 1730 (2006), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and any successor resolutions.

8. For persons and entities designated pursuant to resolution 1373 (2001), countries should have appropriate legal authorities and procedures or mechanisms to delist and unfreeze the funds or other assets of persons and entities that no longer meet the criteria for designation. Countries should also have procedures in place to allow, upon request, review of the designation decision before a court or other independent competent authority.

9. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e. a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of

[7] Security Council resolutions apply to all natural and legal persons within the country.

© 2012-2019

such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

10. Where countries have determined that funds or other assets of persons and entities designated by the Security Council, or one of its relevant sanctions committees, are necessary for basic expenses, for the payment of certain types of fees, expenses and service charges, or for extraordinary expenses, countries should authorise access to such funds or other assets in accordance with the procedures set out in Security Council resolution 1452 (2002) and any successor resolutions. On the same grounds, countries should authorise access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-)national country pursuant to resolution 1373 (2001) and as set out in resolution 1963 (2010).

11. Countries should provide for a mechanism through which a designated person or entity can challenge their designation, with a view to having it reviewed by a competent authority or a court. With respect to designations on the Al-Qaida Sanctions List, countries should inform designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to resolution 1904 (2009), to accept de-listing petitions.

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **Security Council resolutions 1267 (1999), 1989 (2011) and their successor resolutions**[8]:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof[9]; or

[8] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267(1999). At the time of issuance of this Interpretive Note, (February 2012) , the successor resolutions to resolution 1267 (1999) are: resolutions 1333 (2000), 1367 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1988 (2011), and 1989 (2011).

[9] OP2 of resolution 1617 (2005) further defines the criteria for being "associated with" Al-Qaida or Usama bin Laden.

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i), or by persons acting on their behalf or at their direction.

(b) **Security Council resolutions 1267 (1999), 1988 (2011) and their successor resolutions**:

(i) any person or entity participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materiel to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or

(ii) any undertaking owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(b)(i) of this subparagraph, or by persons acting on their behalf or at their direction.

(c) **Security Council resolution 1373 (2001)**:

(i) any person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;

(ii) any entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(c) (i) of this subparagraph; or

(iii) any person or entity acting on behalf of, or at the direction of, any person or entity designated under subsection 13(c) (i) of this subparagraph.

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 7 (TARGETED FINANCIAL SANCTIONS RELATED TO PROLIFERATION)

A. OBJECTIVE

1. Recommendation 7 requires countries to implement targeted financial sanctions[10] to comply with United Nations Security Council resolutions that require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds and other assets are made available to, and for the benefit of, any person[11] or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction.[12]

2. It should be stressed that none of the requirements in Recommendation 7 is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding, as is required by international treaties or Security Council resolutions relating to weapons of mass destruction non-proliferation.[13] The focus of Recommendation 7 is on preventive measures that are necessary and unique in the context of stopping the flow of funds or other assets to proliferators or proliferation; and the use of funds or other assets by proliferators or proliferation, as required by the United Nations Security Council (the Security Council).

---

10 Recommendation 7 is focused on targeted financial sanctions. These include the specific restrictions set out in Security Council resolution 2231 (2015) (see Annex B paragraphs 6(c) and (d)). However, it should be noted that the relevant United Nations Security Council Resolutions are much broader and prescribe other types of sanctions (such as travel bans) and other types of financial provisions (such as activity-based financial prohibitions, category-based sanctions and vigilance measures). With respect to targeted financial sanctions related to the financing of proliferation of weapons of mass destruction and other types of financial provisions, the FATF has issued non-binding guidance, which jurisdictions are encouraged to consider in their implementation of the relevant UNSCRs.

11 Natural or legal person.

12 Recommendation 7 is applicable to all current Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction, any future successor resolutions, and any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. At the time of issuance of this Interpretive Note (June 2017), the Security Council resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction are: resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016) and 2356 (2017). Resolution 2231 (2015), endorsing the Joint Comprehensive Plan of Action, terminated all provisions of resolutions relating to Iran and proliferation financing, including 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010), but established specific restrictions including targeted financial sanctions. This lifts sanctions as part of a step by step approach with reciprocal commitments endorsed by the Security Council. Implementation day of the JCPOA was on 16 January 2016.

13 Based on requirements set, for instance, in the *Nuclear Non-Proliferation Treaty*, the *Biological and Toxin Weapons Convention*, the *Chemical Weapons Convention*, and Security Council resolutions 1540 (2004) and 2235 (2016). Those obligations exist separately and apart from the obligations set forth in Recommendation 7 and its interpretive note.

B. DESIGNATIONS

3. Designations are made by the Security Council in annexes to the relevant resolutions, or by the Security Council Committees established pursuant to these resolutions. There is no specific obligation upon United Nations Member States to submit proposals for designations to the Security Council or the relevant Security Council Committee(s). However, in practice, the Security Council or the relevant Committee(s) primarily depends upon requests for designation by Member States. Security Council resolution 1718 (2006) provides that the relevant Committee shall promulgate guidelines as may be necessary to facilitate the implementation of the measures imposed by this resolution and its successor resolutions. Resolution 2231 (2015) provides that the Security Council shall make the necessary practical arrangements to undertake directly tasks related to the implementation of the resolution.

4. Countries could consider establishing the authority and effective procedures or mechanisms to propose persons and entities to the Security Council for designation in accordance with relevant Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. In this regard, countries could consider the following elements:

   (a) identifying a competent authority(ies), either executive or judicial, as having responsibility for:

      (i) proposing to the 1718 Sanctions Committee, for designation as appropriate, persons or entities that meet the specific criteria for designation as set forth in resolution 1718 (2006) and its successor resolutions[14], if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions); and

      (ii) proposing to the Security Council, for designation as appropriate, persons or entities that meet the criteria for designation as set forth in resolution 2231 (2015) and any future successor resolutions, if that authority decides to do so and believes that it has sufficient evidence to support the designation criteria (see Section E for the specific designation criteria associated with relevant Security Council resolutions).

   (b) having a mechanism(s) for identifying targets for designation, based on the designation criteria set out in resolutions 1718 (2006), 2231 (2015), and their successor and any future successor resolutions (see Section E for the specific designation criteria of relevant Security Council resolutions). Such procedures should ensure the determination, according to applicable (supra-)national principles, whether reasonable grounds or a reasonable basis exists to propose a designation.

---

14 Recommendation 7 is applicable to all current and future successor resolutions to resolution 1718 (2006). At the time of issuance of this Interpretive Note (June 2017), the successor resolutions to resolution 1718 (2006) are: resolution 1874 (2009), resolution 2087 (2013), resolution 2094 (2013), resolution 2270 (2016), resolution 2321 (2016) and resolution 2356 (2017).

© 2012-2019

(c) having appropriate legal authority, and procedures or mechanisms, to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions.

(d) when deciding whether or not to propose a designation, taking into account the criteria in Section E of this interpretive note. For proposals of designations, the competent authority of each country will apply the legal standard of its own legal system, taking into consideration human rights, respect for the rule of law, and in recognition of the rights of innocent third parties.

(e) when proposing names to the 1718 Sanctions Committee, pursuant to resolution 1718 (2006) and its successor resolutions, or to the Security Council, pursuant to resolution 2231 (2015) and any future successor resolutions, providing as much detail as possible on:

(i) the proposed name, in particular, sufficient identifying information to allow for the accurate and positive identification of persons and entities; and

(ii) specific information supporting a determination that the person or entity meets the relevant criteria for designation (see Section E for the specific designation criteria of relevant Security Council resolutions).

(f) having procedures to be able, where necessary, to operate ex parte against a person or entity who has been identified and whose proposal for designation is being considered.

C. FREEZING AND PROHIBITING DEALING IN FUNDS OR OTHER ASSETS OF DESIGNATED PERSONS AND ENTITIES

5. There is an obligation for countries to implement targeted financial sanctions without delay against persons and entities designated:

(a) in the case of resolution 1718 (2006) and its successor resolutions, by the Security Council in annexes to the relevant resolutions, or by the 1718 Sanctions Committee of the Security Council[15]; and

(b) in the case of resolution 2231 (2015) and any future successor resolutions by the Security Council,

when acting under the authority of Chapter VII of the Charter of the United Nations.

[15] As noted in resolution 2270 (2016) (OP32) this also applies to entities of the Government of the Democratic People's Republic of Korea or the Worker's Party of Korea that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

6. Countries should establish the necessary legal authority and identify competent domestic authorities responsible for implementing and enforcing targeted financial sanctions, in accordance with the following standards and procedures:

   (a) Countries[16] should require all natural and legal persons within the country to freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. This obligation should extend to: all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

   (b) Countries should ensure that any funds or other assets are prevented from being made available by their nationals or by any persons or entities within their territories, to or for the benefit of designated persons or entities unless licensed, authorised or otherwise notified in accordance with the relevant Security Council resolutions (see Section E below).

   (c) Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

   (d) Countries should require financial institutions and DNFBPs[17] to report to competent authorities any assets frozen or actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions, and ensure that such information is effectively utilised by competent authorities.

   (e) Countries should adopt effective measures which protect the rights of bona fide third parties acting in good faith when implementing the obligations under Recommendation 7.

   (f) Countries should adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions and DNFBPs with the relevant laws or

---

16 In the case of the European Union (EU), which is considered a supra-national jurisdiction under Recommendation 7 by the FATF, the assets of designated persons and entities are frozen under EU Common Foreign and Security Policy (CFSP) Council decisions and Council regulations (as amended). EU member states may have to take additional measures to implement the freeze, and all natural and legal persons within the EU have to respect the freeze and not make funds available to designated persons and entities.

17 Security Council resolutions apply to all natural and legal persons within the country.

© 2012-2019

enforceable means governing the obligations under Recommendation 7. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions.

D. DE-LISTING, UNFREEZING AND PROVIDING ACCESS TO FROZEN FUNDS OR OTHER ASSETS

7. Countries should develop and implement publicly known procedures to submit de-listing requests to the Security Council in the case of designated persons and entities, that, in the view of the country, do not or no longer meet the criteria for designation. Once the Security Council or the relevant Sanctions Committee has de-listed the person or entity, the obligation to freeze no longer exists. In the case of resolution 1718 (2006) and its successor resolutions, such procedures and criteria should be in accordance with any applicable guidelines or procedures adopted by the Security Council pursuant to resolution 1730 (2006) and any successor resolutions, including those of the Focal Point mechanism established under that resolution. Countries should enable listed persons and entities to petition a request for delisting at the Focal Point for de-listing established pursuant to resolution 1730 (2006), or should inform designated persons or entities to petition the Focal Point directly.

8. For persons or entities with the same or similar name as designated persons or entities, who are inadvertently affected by a freezing mechanism (i.e., a false positive), countries should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner, upon verification that the person or entity involved is not a designated person or entity.

9. Where countries have determined that the exemption conditions set out in resolution 1718(2006) and resolution 2231 (2015) are met, countries should authorise access to funds or other assets in accordance with the procedures set out therein.

10. Countries should permit the addition to the accounts frozen pursuant to resolution 1718 (2006) or resolution 2231 (2015) of interests or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that any such interest, other earnings and payments continue to be subject to these provisions and are frozen.

11. Freezing action taken pursuant to resolution 1737 (2006) and continued by resolution 2231 (2015), or taken pursuant to resolution 2231 (2015), shall not prevent a designated person or entity from making any payment due under a contract entered into prior to the listing of such person or entity, provided that:

    (a) the relevant countries have determined that the contract is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in resolution 2231 (2015) and any future successor resolutions;

    (b) the relevant countries have determined that the payment is not directly or indirectly received by a person or entity subject to the measures in paragraph 6 of Annex B to resolution 2231 (2015); and

(c) the relevant countries have submitted prior notification to the Security Council of the intention to make or receive such payments or to authorise, where appropriate, the unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorisation.[18]

12. Countries should have mechanisms for communicating de-listings and unfreezings to the financial sector and the DNFBPs immediately upon taking such action, and providing adequate guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations to respect a de-listing or unfreezing action.

E. UNITED NATIONS DESIGNATION CRITERIA

13. The criteria for designation as specified in the relevant United Nations Security Council resolutions are:

(a) **On DPRK - Resolutions 1718 (2006), 2087 (2013), 2094 (2013) and 2270 (2016)**:

(i) any person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programmes;

(ii) any person or entity providing support for DPRK's nuclear-related, other WMD-related and ballistic missile-related programmes, including through illicit means;

(iii) any person or entity acting on behalf of or at the direction of any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[19];

(iv) any legal person or entity owned or controlled, directly or indirectly, by any person or entity designated under subsection 13(a)(i) or subsection 13(a)(ii)[20];

(v) any person or entity that has assisted in the evasion of sanctions or in violating the provisions of resolutions 1718 (2006) and 1874 (2009);

(vi) any person or entity that has contributed to DPRK's prohibited programmes, activities prohibited by the DPRK-related resolutions, or to the evasion of provisions; or

---

18 In cases where the designated person or entity is a financial institution, jurisdictions should consider the FATF guidance issued as an annex to *The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, adopted in June 2013.*

19 The funds or assets of these persons or entities are frozen regardless of whether they are specifically identified by the Committee. Further, resolution 2270 (2016) OP23 expanded the scope of targeted financial sanctions obligations under resolution 1718 (2006), by applying these to the Ocean Maritime Management Company vessels specified in Annex III of resolution 2270 (2016).

20 Ibid.

© 2012-2019

(vii) any entity of the Government of the DPRK or the Worker's Party of Korea, or person or entity acting on their behalf or at their direction, or by any entity owned or controlled by them, that countries determine are associated with the DPRK's nuclear or ballistic missile programmes or other activities prohibited by resolution 1718 (2006) and successor resolutions.

(b) **On Iran - Resolution 2231 (2015)**:

(i) any person or entity having engaged in, directly associated with or provided support for Iran's proliferation sensitive nuclear activities contrary to Iran's commitments in the Joint Comprehensive Plan of Action (JCPOA) or the development of nuclear weapon delivery systems, including through the involvement in procurement of prohibited items, goods, equipment, materials and technology specified in Annex B to resolution 2231 (2015);

(ii) any person or entity assisting designated persons or entities in evading or acting inconsistently with the JCPOA or resolution 2231 (2015); and

(iii) any person or entity acting on behalf or at a direction of any person or entity in subsection 13(b)(i), subsection 13(b)(ii) and/or subsection 13(b)(iii), or by any entities owned or controlled by them.

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 8 (NON-PROFIT ORGANISATIONS)

A. INTRODUCTION

1. Given the variety of legal forms that non-profit organisations (NPOs) can have, depending on the country, the FATF has adopted a functional definition of NPO. This definition is based on those activities and characteristics of an organisation which put it at risk of terrorist financing abuse, rather than on the simple fact that it is operating on a non-profit basis. For the purposes of this Recommendation, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". Without prejudice to Recommendation 1, this Recommendation only applies to those NPOs which fall within the FATF definition of an NPO. It does not apply to the entire universe of NPOs.

2. NPOs play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The FATF recognises the vital importance of NPOs in providing these important charitable services, as well as the difficulty of providing assistance to those in need, often in high risk areas and conflict zones, and applauds the efforts of NPOs to meet such needs. The FATF also recognises the intent and efforts to date of NPOs to promote transparency within their operations and to prevent terrorist financing abuse, including through the development of programmes aimed at discouraging radicalisation and violent extremism. The ongoing international campaign against terrorist financing has identified cases in which terrorists and terrorist organisations exploit some NPOs in the sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations. As well, there have been cases where terrorists create sham charities or engage in fraudulent fundraising for these purposes. This misuse not only facilitates terrorist activity, but also undermines donor confidence and jeopardises the very integrity of NPOs. Therefore, protecting NPOs from terrorist financing abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs and the donor community. Measures to protect NPOs from potential terrorist financing abuse should be targeted and in line with the risk-based approach. It is also important for such measures to be implemented in a manner which respects countries' obligations under the Charter of the United Nations and international human rights law.

3. Some NPOs may be vulnerable to terrorist financing abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. In some cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate some NPOs and misuse funds and operations to cover for, or support, terrorist activity.

© 2012-2019

B. OBJECTIVES AND GENERAL PRINCIPLES

4. The objective of Recommendation 8 is to ensure that NPOs are not misused by terrorist organisations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes. In this Interpretive Note, the approach taken to achieve this objective is based on the following general principles:

   (a) A risk-based approach applying focused measures in dealing with identified threats of terrorist financing abuse to NPOs is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to terrorist financing abuse, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each country.

   (b) Flexibility in developing a national response to terrorist financing abuse of NPOs is essential, in order to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

   (c) Past and ongoing terrorist financing abuse of NPOs requires countries to adopt effective and proportionate measures, which should be commensurate to the risks identified through a risk-based approach.

   (d) Focused measures adopted by countries to protect NPOs from terrorist financing abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote accountability and engender greater confidence among NPOs, across the donor community and with the general public, that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of accountability, integrity and public confidence in the management and functioning of NPOs are integral to ensuring they cannot be abused for terrorist financing.

   (e) Countries are required to identify and take effective and proportionate action against NPOs that either are exploited by, or knowingly supporting, terrorists or terrorist organisations taking into account the specifics of the case. Countries should aim to prevent and prosecute, as appropriate, terrorist financing and other forms of terrorist support. Where NPOs suspected of, or implicated in, terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should, to the extent reasonably possible, minimise negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by NPOs.

   (f) Developing cooperative relationships among the public and private sectors and with NPOs is critical to understanding NPOs' risks and risk mitigation strategies, raising awareness, increasing effectiveness and fostering capabilities to combat terrorist

financing abuse within NPOs. Countries should encourage the development of academic research on, and information-sharing in, NPOs to address terrorist financing related issues.

C. MEASURES

5. Without prejudice to the requirements of Recommendation 1, since not all NPOs are inherently high risk (and some may represent little or no risk at all), countries should identify which subset of organisations fall within the FATF definition of NPO. In undertaking this exercise, countries should use all relevant sources of information in order to identify features and types of NPOs, which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse.[21] It is also crucial to identify the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs. Countries should review the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for terrorism financing support in order to be able to take proportionate and effective actions to address the risks identified. These exercises could take a variety of forms and may or may not be a written product. Countries should also periodically reassess the sector by reviewing new information on the sector's potential vulnerabilities to terrorist activities to ensure effective implementation of measures.

6. There is a diverse range of approaches in identifying, preventing and combating terrorist financing abuse of NPOs. An effective approach should involve all four of the following elements: (a) sustained outreach, (b) targeted risk-based supervision or monitoring, (c) effective investigation and information gathering and (d) effective mechanisms for international cooperation. The following measures represent examples of specific actions that countries should take with respect to each of these elements, in order to protect NPOs from potential terrorist financing abuse.

   (a) Sustained outreach concerning terrorist financing issues

      (i) Countries should have clear policies to promote accountability, integrity and public confidence in the administration and management of NPOs.

      (ii) Countries should encourage and undertake outreach and educational programmes to raise and deepen awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks, and the measures that NPOs can take to protect themselves against such abuse.

      (iii) Countries should work with NPOs to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect them from terrorist financing abuse.

[21] For example, such information could be provided by regulators, tax authorities, FIUs, donor organisations or law enforcement and intelligence authorities.

© 2012-2019

(iv) Countries should encourage NPOs to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

(b) Targeted risk-based supervision or monitoring of NPOs

Countries should take steps to promote effective supervision or monitoring. A "one-size-fits-all" approach would be inconsistent with the proper implementation of a risk-based approach as stipulated under Recommendation 1 of the FATF Standards. In practice, countries should be able to demonstrate that risk-based measures apply to NPOs at risk of terrorist financing abuse. It is also possible that existing regulatory or other measures may already sufficiently address the current terrorist financing risk to the NPOs in a jurisdiction, although terrorist financing risks to the sector should be periodically reviewed. Appropriate authorities should monitor the compliance of NPOs with the requirements of this Recommendation, including the risk-based measures being applied to them.[22] Appropriate authorities should be able to apply effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.[23] The following are some examples of measures that could be applied to NPOs, in whole or in part, depending on the risks identified:

(i) NPOs could be required to license or register. This information should be available to competent authorities and encouraged to be available to the public.[24]

(ii) NPOs could be required to maintain information on: (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information could be publicly available either directly from the NPO or through appropriate authorities.

(iii) NPOs could be required to issue annual financial statements that provide detailed breakdowns of incomes and expenditures.

(iv) NPOs could be required to have appropriate controls in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of the NPO's stated activities.

(v) NPOs could be required to take reasonable measures to confirm the identity, credentials and good standing of beneficiaries[25] and associate NPOs and that

22 In this context, rules and regulations may include rules and standards applied by self-regulatory organisations and accrediting institutions.

23 The range of such sanctions might include freezing of accounts, removal of trustees, fines, de-certification, de-licensing and de-registration. This should not preclude parallel civil, administrative or criminal proceedings with respect to NPOs or persons acting on their behalf where appropriate.

24 Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, NPOs are already registered with tax authorities and monitored in the context of qualifying for favourable tax treatment (such as tax credits or tax exemptions).

they are not involved with and/or using the charitable funds to support terrorists or terrorist organisations[26]. However, NPOs should not be required to conduct customer due diligence. NPOs could be required to take reasonable measures to document the identity of their significant donors and to respect donor confidentiality. The ultimate objective of this requirement is to prevent charitable funds from being used to finance and support terrorists and terrorist organisations.

(vi) NPOs could be required to maintain, for a period of at least five years, records of domestic and international transactions that are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the organisation, and could be required to make these available to competent authorities upon appropriate authority. This also applies to information mentioned in paragraphs (ii) and (iii) above. Where appropriate, records of charitable activities and financial operations by NPOs could also be made available to the public.

(c) Effective information gathering and investigation

(i) Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs.

(ii) Countries should have investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations.

(iii) Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.

(iv) Countries should establish appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO: (1) is involved in terrorist financing abuse and/or is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures, or other forms of terrorist support; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, that this information is promptly shared with relevant competent authorities, in order to take preventive or investigative action.

---

25 The term beneficiaries refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.

26 This does not mean that NPOs are expected to identify each specific individual, as such a requirement would not always be possible and would, in some instances, impede the ability of NPOs to provide much-needed services

© 2012-2019

(d) Effective capacity to respond to international requests for information about an NPO of concern. Consistent with Recommendations on international cooperation, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support.

D. RESOURCES FOR SUPERVISION, MONITORING, AND INVESTIGATION

7. Countries should provide their appropriate authorities, which are responsible for supervision, monitoring and investigation of their NPO sector, with adequate financial, human and technical resources.

Glossary of specific terms used in this Recommendation	
Appropriate authorities	refers to competent authorities, including regulators, tax authorities, FIUs, law enforcement, intelligence authorities, accrediting institutions, and potentially self-regulatory organisations in some jurisdictions.
Associate NPOs	includes foreign branches of international NPOs, and NPOs with which partnerships have been arranged.
Beneficiaries	refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO.
Non-profit organisation or NPO	refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".
Terrorist financing abuse	refers to the exploitation by terrorists and terrorist organisations of NPOs to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support terrorists or terrorist organisations and operations.

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE)

A. CUSTOMER DUE DILIGENCE AND TIPPING-OFF

1. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

   (a) normally seek to identify and verify the identity[27] of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply; and

   (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.

2. Recommendation 21 prohibits financial institutions, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to the FIU. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

3. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD.

B. CDD – PERSONS ACTING ON BEHALF OF A CUSTOMER

4. When performing elements (a) and (b) of the CDD measures specified under Recommendation 10, financial institutions should also be required to verify that any person purporting to act on behalf of the customer is so authorised, and should identify and verify the identity of that person.

C. CDD FOR LEGAL PERSONS AND ARRANGEMENTS

5. When performing CDD measures in relation to customers that are legal persons or legal arrangements[28], financial institutions should be required to identify and verify the identity of

---

[27] Reliable, independent source documents, data or information will hereafter be referred to as "identification data."

[28] In these Recommendations references to legal arrangements such as trusts (or other similar arrangements) being the customer of a financial institution or DNFBP or carrying out a transaction, refers to situations where a natural or legal person that is the trustee establishes the business relationship or carries out the transaction on the behalf of the beneficiaries or according to the terms of the trust. The normal CDD requirements for customers that are natural or legal persons would continue

© 2012-2019

the customer, and understand the nature of its business, and its ownership and control structure. The purpose of the requirements set out in (a) and (b) below, regarding the identification and verification of the customer and the beneficial owner, is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, financial institutions should be required to:

(a) Identify the customer and verify its identity. The type of information that would normally be needed to perform this function would be:

(i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

(ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

(iii) The address of the registered office, and, if different, a principal place of business.

(b) Identify the beneficial owners of the customer and take reasonable measures[29] to verify the identity of such persons, through the following information:

(i) For legal persons[30]:

(i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest[31] in a legal person; and

---

to apply, including paragraph 4 of INR.10, but the additional requirements regarding the trust and the beneficial owners of the trust (as defined) would also apply.

29 In determining the reasonableness of the identity verification measures, regard should be had to the money laundering and terrorist financing risks posed by the customer and the business relationship.

30 Measures (i.i) to (i.iii) are not alternative options, but are cascading measures, with each to be used where the previous measure has been applied and has not identified a beneficial owner.

31 A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%).

(i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, financial institutions should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

(ii) For legal arrangements:

(ii.i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries[32], and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

(ii.ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

D. CDD FOR BENEFICIARIES OF LIFE INSURANCE POLICIES

6. For life or other investment-related insurance business, financial institutions should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the

[32] For beneficiary(ies) of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

© 2012-2019

financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

The information collected under (a) and/or (b) should be recorded and maintained in accordance with the provisions of Recommendation 11.

7. For both the cases referred to in 6(a) and (b) above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

8. The beneficiary of a life insurance policy should be included as a relevant risk factor by the financial institution in determining whether enhanced CDD measures are applicable. If the financial institution determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

9. Where a financial institution is unable to comply with paragraphs 6 to 8 above, it should consider making a suspicious transaction report.

E. RELIANCE ON IDENTIFICATION AND VERIFICATION ALREADY PERFORMED

10. The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead an institution to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

F. TIMING OF VERIFICATION

11. Examples of the types of circumstances (in addition to those referred to above for beneficiaries of life insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.

12. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

G. EXISTING CUSTOMERS

13. Financial institutions should be required to apply CDD measures to existing customers[33] on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

H. RISK BASED APPROACH[34]

14. The examples below are not mandatory elements of the FATF Standards, and are included for guidance only. The examples are not intended to be comprehensive, and although they are considered to be helpful indicators, they may not be relevant in all circumstances.

Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(a) Customer risk factors:

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Business that are cash-intensive.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:[35]

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.

---

33 Existing customers as at the date that the national requirements are brought into force.

34 The RBA does not apply to the circumstances when CDD should be required but may be used to determine the extent of such measures.

35 Under Recommendation 19 it is mandatory for countries to require financial institutions to apply enhanced due diligence when the FATF calls for such measures to be introduced.

© 2012-2019

- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Anonymous transactions (which may include cash).
- Non-face-to-face business relationships or transactions.
- Payment received from unknown or un-associated third parties

Lower risks

16. There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the country or by the financial institution, it could be reasonable for a country to allow its financial institutions to apply simplified CDD measures.

17. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

(a) Customer risk factors:

- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.

(b) Product, service, transaction or delivery channel risk factors:

- Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, countries or financial institutions could, when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

18. Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

Risk variables

19. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, a financial institution should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. Examples of such variables include:

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

© 2012-2019

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures

21. Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Thresholds

22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Ongoing due diligence

23. Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 12 (POLITICALLY EXPOSED PERSONS)

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the payout. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

a) inform senior management before the payout of the policy proceeds; and

b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATION 13 (CORRESPONDENT BANKING)

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

The term *payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 14 (MONEY OR VALUE TRANSFER SERVICES)

A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform money or value transfer services, and which are already subject to the full range of applicable obligations under the FATF Recommendations.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATION 15

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value." Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)

2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created[36]. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.

4. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk- based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

[36] References to creating a legal person include incorporation of companies or any other mechanism that is used.

© 2012-2019

6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

7. With respect to the preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:

(a) R. 10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.
(b) R. 16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information[37] on virtual asset transfers, submit[38] the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

8. Countries should rapidly, constructively, and effectively provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

[37] As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context.

[38] The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers.

INTERPRETIVE NOTE TO RECOMMENDATION 16 (WIRE TRANSFERS)

A. OBJECTIVE

1. Recommendation 16 was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator and beneficiary of wire transfers is immediately available:

   (a) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, and prosecuting terrorists or other criminals, and tracing their assets;

   (b) to financial intelligence units for analysing suspicious or unusual activity, and disseminating it as necessary, and

   (c) to ordering, intermediary and beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions, and to implement the requirements to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.

2. To accomplish these objectives, countries should have the ability to trace all wire transfers. Due to the potential terrorist financing threat posed by small wire transfers, countries should minimise thresholds taking into account the risk of driving transactions underground and the importance of financial inclusion. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system.

B. SCOPE

3. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers , including serial payments, and cover payments.

4. Recommendation 16 is not intended to cover the following types of payments:

   (a) Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person wire transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.

   (b) Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

© 2012-2019

5. Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply:

   (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer.

   (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.

C. CROSS-BORDER QUALIFYING WIRE TRANSFERS

6. Information accompanying all qualifying wire transfers should always contain:

   (a) the name of the originator;

   (b) the originator account number where such an account is used to process the transaction;

   (c) the originator's address, or national identity number, or customer identification number[39], or date and place of birth;

   (d) the name of the beneficiary; and

   (e) the beneficiary account number where such an account is used to process the transaction.

7. In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

8. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of paragraph 6 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in paragraph 7 above), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

D. DOMESTIC WIRE TRANSFERS

9. Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter

[39] The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number referred to in paragraph 7. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

10. The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

E. RESPONSIBILITIES OF ORDERING, INTERMEDIARY AND BENEFICIARY FINANCIAL INSTITUTIONS

Ordering financial institution

11. The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information.

12. The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.

13. The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.

14. The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above.

Intermediary financial institution

15. For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it

16. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.

17. An intermediary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

18. An intermediary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

© 2012-2019

Beneficiary financial institution

19. A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

20. For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.

21. A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.

F. MONEY OR VALUE TRANSFER SERVICE OPERATORS

22. Money or value transfer service (MVTS) providers should be required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider:

    (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

    (b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

Glossary of specific terms used in this Recommendation

Accurate	is used to describe information that has been verified for accuracy.
Batch transfer	is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons.
Beneficiary	refers to the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
Beneficiary Financial Institution	refers to the financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary.
Cover Payment	refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution

Glossary of specific terms used in this Recommendation	
	through one or more intermediary financial institutions.
Cross-border wire transfer	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of *wire transfer* in which at least one of the financial institutions involved is located in a different country.
Domestic wire transfers	refers to any *wire transfer* where the ordering financial institution and beneficiary financial institution are located in the same country. This term therefore refers to any chain of *wire transfer* that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country. The term also refers to any chain of *wire transfer* that takes place entirely within the borders of the European Economic Area (EEA)[40].
Intermediary financial institution	refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.
Ordering financial institution	refers to the financial institution which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.
Originator	refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.
Qualifying wire transfers	means a cross-border wire transfer above any applicable threshold as described in paragraph 5 of the Interpretive Note to Recommendation 16.
Required	is used to describe a situation in which all elements of required information are present. Subparagraphs 6(a), 6(b) and 6(c) set out the *required originator information.* Subparagraphs 6(d) and 6(e) set out the *required beneficiary information.*

[40] An entity may petition the FATF to be designated as a supra-national jurisdiction for the purposes of and limited to an assessment of Recommendation 16 compliance.

© 2012-2019

Glossary of specific terms used in this Recommendation	
Serial Payment	refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g. correspondent banks).
Straight-through processing	refers to payment transactions that are conducted electronically without the need for manual intervention.
Unique transaction reference number	refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.
Wire transfer	refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.[41]

[41] It is understood that the settlement of wire transfers may happen under a net settlement arrangement. This interpretive note refers to information which must be included in instructions sent from an originating financial institution to a beneficiary financial institution, including through any intermediary financial institution, to enable disbursement of the funds to the recipient. Any net settlement between the financial institutions may be exempt under paragraph 4(b).

INTERPRETIVE NOTE TO RECOMMENDATION 17 (RELIANCE ON THIRD PARTIES)

1. This Recommendation does not apply to outsourcing or agency relationships. In a third-party reliance scenario, the third party should be subject to CDD and record-keeping requirements in line with Recommendations 10 and 11, and be regulated, supervised or monitored. The third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control of the effective implementation of those procedures by the outsourced entity.

2. For the purposes of Recommendation 17, the term *relevant competent authorities* means (i) the home authority, that should be involved for the understanding of group policies and controls at group-wide level, and (ii) the host authorities, that should be involved for the branches/subsidiaries.

3. The term *third parties* means financial institutions or DNFBPs that are supervised or monitored and that meet the requirements under Recommendation 17.

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 18 (INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES)

1. Financial institutions' programmes against money laundering and terrorist financing should include:

   (a) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;

   (b) an ongoing employee training programme; and

   (c) an independent audit function to test the system.

2. The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

3. Compliance management arrangements should include the appointment of a compliance officer at the management level.

4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management.

5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial

group, including, as appropriate, requesting the financial group to close down its operations in the host country.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 19 (HIGHER-RISK COUNTRIES)

1. The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.

2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:

   (a) Requiring financial institutions to apply specific elements of enhanced due diligence.

   (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.

   (c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.

   (d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems.

   (e) Limiting business relationships or financial transactions with the identified country or persons in that country.

   (f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.

   (g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.

   (h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.

   (i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

   There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries

INTERPRETIVE NOTE TO RECOMMENDATION 20 (REPORTING OF SUSPICIOUS TRANSACTIONS)

1. The reference to criminal activity in Recommendation 20 refers to all criminal acts that would constitute a predicate offence for money laundering or, at a minimum, to those offences that would constitute a predicate offence, as required by Recommendation 3. Countries are strongly encouraged to adopt the first of these alternatives.

2. The reference to terrorist financing in Recommendation 20 refers to: the financing of terrorist acts and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.

3. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called "indirect reporting"), is not acceptable.

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATIONS 22 AND 23 (DNFBPS)

1. The designated thresholds for transactions are as follows:

   - Casinos (under Recommendation 22) - USD/EUR 3,000
   - For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 22 and 23) - USD/EUR 15,000.

   Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

2. The Interpretive Notes that apply to financial institutions are also relevant to DNFBPs, where applicable. To comply with Recommendations 22 and 23, countries do not need to issue laws or enforceable means that relate exclusively to lawyers, notaries, accountants and the other designated non-financial businesses and professions, so long as these businesses or professions are included in laws or enforceable means covering the underlying activities.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATION 22 (DNFBPS – CUSTOMER DUE DILIGENCE)

1. Real estate agents should comply with the requirements of Recommendation 10 with respect to both the purchasers and vendors of the property.

2. Casinos should implement Recommendation 10, including identifying and verifying the identity of customers, when their customers engage in financial transactions equal to or above USD/EUR 3,000. Conducting customer identification at the entry to a casino could be, but is not necessarily, sufficient. Countries must require casinos to ensure that they are able to link customer due diligence information for a particular customer to the transactions that the customer conducts in the casino.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 23 (DNFBPS – OTHER MEASURES)

1. Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report suspicious transactions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

2. It is for each country to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings.

3. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of cooperation between these organisations and the FIU.

4. Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 24 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS)

1. Competent authorities should be able to obtain, or have access in a timely fashion to, adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons (beneficial ownership information[42]) that are created[43] in the country. Countries may choose the mechanisms they rely on to achieve this objective, although they should also comply with the minimum requirements set out below. It is also very likely that countries will need to utilise a combination of mechanisms to achieve the objective.

2. As part of the process of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:

   (a) identify and describe the different types, forms and basic features of legal persons in the country.

   (b) identify and describe the processes for: (i) the creation of those legal persons; and (ii) the obtaining and recording of basic and beneficial ownership information;

   (c) make the above information publicly available; and

   (d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country.

A. BASIC INFORMATION

3. In order to determine who the beneficial owners of a company are, competent authorities will require certain basic information about the company, which, at a minimum, would include information about the legal ownership and control structure of the company. This would include information about the status and powers of the company, its shareholders and its directors.

4. All companies created in a country should be registered in a company registry.[44] Whichever combination of mechanisms is used to obtain and record beneficial ownership information (see section B), there is a set of basic information on a company that needs to be obtained and recorded by the company[45] as a necessary prerequisite. The minimum basic information to be obtained and recorded by a company should be:

---

42 Beneficial ownership information for legal persons is the information referred to in the interpretive note to Recommendation 10, paragraph 5(b)(i). Controlling shareholders as referred to in, paragraph 5(b)(i) of the interpretive note to Recommendation 10 may be based on a threshold, e.g. any persons owning more than a certain percentage of the company (e.g. 25%).

43 References to creating a legal person, include incorporation of companies or any other mechanism that is used.

44 "Company registry" refers to a register in the country of companies incorporated or licensed in that country and normally maintained by or for the incorporating authority. It does not refer to information held by or for the company itself.

45 The information can be recorded by the company itself or by a third person under the company's responsibility.

© 2012-2019

(a) company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors; and

(b) a register of its shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder[46] and categories of shares (including the nature of the associated voting rights).

5. The company registry should record all the basic information set out in paragraph 4(a) above.

6. The company should maintain the basic information set out in paragraph 4(b) within the country, either at its registered office or at another location notified to the company registry. However, if the company or company registry holds beneficial ownership information within the country, then the register of shareholders need not be in the country, provided that the company can provide this information promptly on request.

B. BENEFICIAL OWNERSHIP INFORMATION

7. Countries should ensure that either: (a) information on the beneficial ownership of a company is obtained by that company and available at a specified location in their country; or (b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority.

8. In order to meet the requirements in paragraph 7, countries should use one or more of the following mechanisms:

(a) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

(b) Requiring companies to take reasonable measures[47] to obtain and hold up-to-date information on the companies' beneficial ownership;

(c) Using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22[48]; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (e.g. company registries, tax authorities or financial or other regulators); (iii) information held by the company as required above in Section A; and (iv) available information on companies listed on a stock exchange, where disclosure requirements (either by stock exchange rules or through law or enforceable means) impose requirements to ensure adequate transparency of beneficial ownership.

---

46 This is applicable to the nominal owner of all registered shares.

47 Measures taken should be proportionate to the level of risk or complexity induced by the ownership structure of the company or the nature of the controlling shareholders.

48 Countries should be able to determine in a timely manner whether a company has an account with a financial institution within the country.

9. Regardless of which of the above mechanisms are used, countries should ensure that companies cooperate with competent authorities to the fullest extent possible in determining the beneficial owner. This should include:

   (a) Requiring that one or more natural persons resident in the country is authorised by the company[49], and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

   (b) Requiring that a DNFBP in the country is authorised by the company, and accountable to competent authorities, for providing all basic information and available beneficial ownership information, and giving further assistance to the authorities; and/or

   (c) Other comparable measures, specifically identified by the country, which can effectively ensure cooperation.

10. All the persons, authorities and entities mentioned above, and the company itself (or its administrators, liquidators or other persons involved in the dissolution of the company), should maintain the information and records referred to for at least five years after the date on which the company is dissolved or otherwise ceases to exist, or five years after the date on which the company ceases to be a customer of the professional intermediary or the financial institution.

C. TIMELY ACCESS TO CURRENT AND ACCURATE INFORMATION

11. Countries should have mechanisms that ensure that basic information, including information provided to the company registry, is accurate and updated on a timely basis. Countries should require that any available information referred to in paragraph 7 is accurate and is kept as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.

12. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

13. Countries should require their company registry to facilitate timely access by financial institutions, DNFBPs and other countries' competent authorities to the public information they hold, and, at a minimum to the information referred to in paragraph 4(a) above. Countries should also consider facilitating timely access by financial institutions and DNFBPs to information referred to in paragraph 4(b) above.

D. OBSTACLES TO TRANSPARENCY

14. Countries should take measures to prevent the misuse of bearer shares and bearer share warrants, for example by applying one or more of the following mechanisms: (a) prohibiting

[49] Members of the company's board or senior management may not require specific authorisation by the company.

© 2012-2019

them; (b) converting them into registered shares or share warrants (for example through dematerialisation); (c) immobilising them by requiring them to be held with a regulated financial institution or professional intermediary; or (d) requiring shareholders with a controlling interest to notify the company, and the company to record their identity.

15. Countries should take measures to prevent the misuse of nominee shares and nominee directors, for example by applying one or more of the following mechanisms: (a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register; or (b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request.

E. OTHER LEGAL PERSONS

16. In relation to foundations, Anstalt, and limited liability partnerships, countries should take similar measures and impose similar requirements, as those required for companies, taking into account their different forms and structures.

17. As regards other types of legal persons, countries should take into account the different forms and structures of those other legal persons, and the levels of money laundering and terrorist financing risks associated with each type of legal person, with a view to achieving appropriate levels of transparency. At a minimum, countries should ensure that similar types of basic information should be recorded and kept accurate and current by such legal persons, and that such information is accessible in a timely way by competent authorities. Countries should review the money laundering and terrorist financing risks associated with such other legal persons, and, based on the level of risk, determine the measures that should be taken to ensure that competent authorities have timely access to adequate, accurate and current beneficial ownership information for such legal persons.

F. LIABILITY AND SANCTIONS

18. There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability and effective, proportionate and dissuasive sanctions, as appropriate for any legal or natural person that fails to properly comply with the requirements.

G. INTERNATIONAL COOPERATION

19. Countries should rapidly, constructively and effectively provide international cooperation in relation to basic and beneficial ownership information, on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers, in accordance with their domestic law, to obtain beneficial ownership information on behalf of foreign counterparts. Countries should monitor

the quality of assistance they receive from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 25 (TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS)

1. Countries should require trustees of any express trust governed under their law to obtain and hold adequate, accurate, and current beneficial ownership information regarding the trust. This should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. Countries should also require trustees of any trust governed under their law to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors.

2. All countries should take measures to ensure that trustees disclose their status to financial institutions and DNFBPs when, as a trustee, forming a business relationship or carrying out an occasional transaction above the threshold. Trustees should not be prevented by law or enforceable means from providing competent authorities with any information relating to the trust[50]; or from providing financial institutions and DNFBPs, upon request, with information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business relationship.

3. Countries are encouraged to ensure that other relevant authorities, persons and entities hold information on all trusts with which they have a relationship. Potential sources of information on trusts, trustees, and trust assets are:

   (a) Registries (e.g. a central registry of trusts or trust assets), or asset registries for land, property, vehicles, shares or other assets.

   (b) Other competent authorities that hold information on trusts and trustees (e.g. tax authorities which collect information on assets and income relating to trusts).

   (c) Other agents and service providers to the trust, including investment advisors or managers, lawyers, or trust and company service providers.

4. Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to obtain timely access to the information held by trustees and other parties, in particular information held by financial institutions and DNFBPs on: (a) the beneficial ownership; (b) the residence of the trustee; and (c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

5. Professional trustees should be required to maintain the information referred to in paragraph 1 for at least five years after their involvement with the trust ceases. Countries are encouraged to require non-professional trustees and the other authorities, persons and entities mentioned in paragraph 3 above to maintain the information for at least five years.

---

50 Domestic competent authorities or the relevant competent authorities of another country pursuant to an appropriate international cooperation request.

6. Countries should require that any information held pursuant to paragraph 1 above should be kept accurate and be as current and up-to-date as possible, and the information should be updated within a reasonable period following any change.

7. Countries should consider measures to facilitate access to any information on trusts that is held by the other authorities, persons and entities referred to in paragraph 3, by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

8. In the context of this Recommendation, countries are not required to give legal recognition to trusts. Countries need not include the requirements of paragraphs 1, 2 and 6 in legislation, provided that appropriate obligations to such effect exist for trustees (e.g. through common law or case law).

Other Legal Arrangements

9. As regards other types of legal arrangement with a similar structure or function, countries should take similar measures to those required for trusts, with a view to achieving similar levels of transparency. At a minimum, countries should ensure that information similar to that specified above in respect of trusts should be recorded and kept accurate and current, and that such information is accessible in a timely way by competent authorities.

International Cooperation

10. Countries should rapidly, constructively and effectively provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements on the basis set out in Recommendations 37 and 40. This should include (a) facilitating access by foreign competent authorities to any information held by registries or other domestic authorities; (b) exchanging domestically available information on the trusts or other legal arrangement; and (c) using their competent authorities' powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.

Liability and Sanctions

11. Countries should ensure that there are clear responsibilities to comply with the requirements in this Interpretive Note; and that trustees are either legally liable for any failure to perform the duties relevant to meeting the obligations in paragraphs 1, 2, 6 and (where applicable) 5; or that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to comply.[51] Countries should ensure that there are effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to

[51] This does not affect the requirements for effective, proportionate, and dissuasive sanctions for failure to comply with requirements elsewhere in the Recommendations.

© 2012-2019

grant to competent authorities timely access to information regarding the trust referred to in paragraphs 1 and 5.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATION 26 (REGULATION AND SUPERVISION OF FINANCIAL INSTITUTIONS)

Risk-based approach to Supervision

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising institutions that apply an AML/CFT risk-based approach.

2. Adopting a risk-based approach to supervising financial institutions' AML/CFT systems and controls allows supervisory authorities to shift resources to those areas that are perceived to present higher risk. As a result, supervisory authorities can use their resources more effectively. This means that supervisors: (a) should have a clear understanding of the money laundering and terrorist financing risks present in a country; and (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group (or groups, when applicable for Core Principles institutions). The frequency and intensity of on-site and off-site AML/CFT supervision of financial institutions/groups should be based on the money laundering and terrorist financing risks, and the policies, internal controls and procedures associated with the institution/group, as identified by the supervisor's assessment of the institution/group's risk profile, and on the money laundering and terrorist financing risks present in the country.

3. The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group, in accordance with the country's established practices for ongoing supervision. This assessment should not be static: it will change depending on how circumstances develop and how threats evolve.

4. AML/CFT supervision of financial institutions/groups that apply a risk-based approach should take into account the degree of discretion allowed under the RBA to the financial institution/group, and encompass, in an appropriate manner, a review of the risk assessments underlying this discretion, and of the adequacy and implementation of its policies, internal controls and procedures.

5. These principles should apply to all financial institutions/groups. To ensure effective AML/CFT supervision, supervisors should take into consideration the characteristics of the financial institutions/groups, in particular the diversity and number of financial institutions, and the degree of discretion allowed to them under the RBA.

Resources of supervisors

6. Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and

© 2012-2019

autonomy to ensure freedom from undue influence or interference. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATION 28 (REGULATION AND SUPERVISION OF DNFBPS)

1. Risk-based approach to supervision refers to: (a) the general process by which a supervisor or SRB, according to its understanding of risks, allocates its resources to AML/CFT supervision; and (b) the specific process of supervising or monitoring DNFBPs that apply an AML/CFT risk-based approach.

2. Supervisors or SRBs should determine the frequency and intensity of their supervisory or monitoring actions on DNFBPs on the basis of their understanding of the money laundering and terrorist financing risks, and taking into consideration the characteristics of the DNFBPs, in particular their diversity and number, in order to ensure effective AML/CFT supervision or monitoring. This means having a clear understanding of the money laundering and terrorist financing risks: (a) present in the country; and (b) associated with the type of DNFBP and their customers, products and services.

3. Supervisors or SRBs assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs should properly take into account the money laundering and terrorist financing risk profile of those DNFBPs, and the degree of discretion allowed to them under the RBA.

4. Supervisors or SRBs should have adequate powers to perform their functions (including powers to monitor and sanction), and adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 29 (FINANCIAL INTELLIGENCE UNITS)

A. GENERAL

1. This note explains the core mandate and functions of a financial intelligence unit (FIU) and provides further clarity on the obligations contained in the standard. The FIU is part of, and plays a central role in, a country's AML/CFT operational network, and provides support to the work of other competent authorities. Considering that there are different FIU models, Recommendation 29 does not prejudge a country's choice for a particular model, and applies equally to all of them.

B. FUNCTIONS

(a) Receipt

2. The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

(b) Analysis

3. FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received, and on the expected use after dissemination. FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. However, such tools cannot fully replace the human judgement element of analysis. FIUs should conduct the following types of analysis:

- Operational analysis uses available and obtainable information to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing.
- Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns. This information is then also used by the FIU or other state entities in order to determine money laundering and terrorist financing related threats and vulnerabilities. Strategic analysis may also help establish policies and goals for the FIU, or more broadly for other entities within the AML/CFT regime.

(c) Dissemination

4. The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities. Dedicated, secure and protected channels should be used for the dissemination.

- **Spontaneous dissemination**: The FIU should be able to disseminate information and the results of its analysis to competent authorities when there are grounds to suspect money laundering, predicate offences or terrorist financing. Based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information.
- **Dissemination upon request:** The FIU should be able to respond to information requests from competent authorities pursuant to Recommendation 31. When the FIU receives such a request from a competent authority, the decision on conducting analysis and/or dissemination of information to the requesting authority should remain with the FIU.

C. ACCESS TO INFORMATION

(a) Obtaining Additional Information from Reporting Entities

5. In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).

(b) Access to Information from other sources

6. In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate, commercially held data.

D. INFORMATION SECURITY AND CONFIDENTIALITY

7. Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations. An FIU must, therefore, have rules in place governing the security and confidentiality of such information, including procedures for handling, storage, dissemination, and protection of, as well as access to such information. The FIU should ensure that its staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. The FIU should ensure that there is limited access to its facilities and information, including information technology systems.

© 2012-2019

E. OPERATIONAL INDEPENDENCE

8. The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information. In all cases, this means that the FIU has the independent right to forward or disseminate information to competent authorities.

9. An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority.

10. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

11. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.

F. UNDUE INFLUENCE OR INTERFERENCE

12. The FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

G. EGMONT GROUP

13. Countries should ensure that the FIU has regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs). The FIU should apply for membership in the Egmont Group.

H. LARGE CASH TRANSACTION REPORTING

14. Countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount.

INTERPRETIVE NOTE TO RECOMMENDATION 30 (RESPONSIBILITIES OF LAW ENFORCEMENT AND INVESTIGATIVE AUTHORITIES)

1. There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation. Countries should also designate one or more competent authorities to identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation.

2. A 'financial investigation' means an enquiry into the financial affairs related to a criminal activity, with a view to:

   - identifying the extent of criminal networks and/or the scale of criminality;
   - identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and
   - developing evidence which can be used in criminal proceedings.

3. A 'parallel financial investigation' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations.

4. Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering and terrorist financing cases to postpone or waive the arrest of suspected persons and/or the seizure of the money, for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

5. Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, *per se*, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

6. Anti-corruption enforcement authorities with enforcement powers may be designated to investigate money laundering and terrorist financing offences arising from, or related to, corruption offences under Recommendation 30, and these authorities should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

7. The range of law enforcement agencies and other competent authorities mentioned above should be taken into account when countries make use of multi-disciplinary groups in financial investigations.

8. Law enforcement authorities and prosecutorial authorities should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the

© 2012-2019

staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATION 32 (CASH COURIERS)

A. OBJECTIVES

1. Recommendation 32 was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures to: (a) detect the physical cross-border transportation of currency and bearer negotiable instruments; (b) stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (c) stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (d) apply appropriate sanctions for making a false declaration or disclosure; and (e) enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.

B. THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

2. Countries may meet their obligations under Recommendation 32 and this Interpretive Note by implementing one of the following types of systems. However, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

Declaration system

3. All persons making a physical cross-border transportation of currency or bearer negotiable instruments (BNIs), which are of a value exceeding a pre-set, maximum threshold of USD/EUR 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries may opt from among the following three different types of declaration system: (i) a written declaration system for all travellers; (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above a threshold; and (iii) an oral declaration system. These three systems are described below in their pure form. However, it is not uncommon for countries to opt for a mixed system.

(a) *Written declaration system for all travellers*: In this system, all travellers are required to complete a written declaration before entering the country. This would include questions contained on common or customs declaration forms. In practice, travellers have to make a declaration whether or not they are carrying currency or BNIs (e.g. ticking a "yes" or "no" box).

(b) *Written declaration system for travellers carrying amounts above a threshold:* In this system, all travellers carrying an amount of currency or BNIs above a pre-set designated threshold are required to complete a written declaration form. In practice, the traveller is not required to fill out any forms if they are not carrying currency or BNIs over the designated threshold.

© 2012-2019

(c) *Oral declaration system for all travellers:* In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. Usually, this is done at customs entry points by requiring travellers to choose between the "red channel" (goods to declare) and the "green channel" (nothing to declare). The choice of channel that the traveller makes is considered to be the oral declaration. In practice, travellers do not declare in writing, but are required to actively report to a customs official.

Disclosure system

4. Countries may opt for a system whereby travellers are required to provide the authorities with appropriate information upon request. In such systems, there is no requirement for travellers to make an upfront written or oral declaration. In practice, travellers need to be required to give a truthful answer to competent authorities upon request.

C. ADDITIONAL ELEMENTS APPLICABLE TO BOTH SYSTEMS

5. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

(a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and BNIs.

(b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs and their intended use.

(c) Information obtained through the declaration/disclosure process should be available to the FIU, either through a system whereby the FIU is notified about suspicious cross-border transportation incidents, or by making the declaration/disclosure information directly available to the FIU in some other way.

(d) At the domestic level, countries should ensure that there is adequate coordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

(e) In the following two cases, competent authorities should be able to stop or restrain cash or BNIs for a reasonable time, in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

(f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Recommendations 36 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure which exceeds the maximum threshold of USD/EUR 15,000 is made; or (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of

money laundering or terrorist financing, this information shall be retained for use by competent authorities. At a minimum, this information will cover: (i) the amount of currency or BNIs declared, disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

(g) Countries should implement Recommendation 32 subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements, in any way.

D. SANCTIONS

6. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or BNIs that is related to terrorist financing, money laundering or predicate offences should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, consistent with Recommendation 4, which would enable the confiscation of such currency or BNIs.

7. Authorities responsible for implementation of Recommendation 32 should have adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of these authorities maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled.

E. GOLD, PRECIOUS METALS AND PRECIOUS STONES

8. For the purposes of Recommendation 32, gold, precious metals and precious stones are not included, despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items, and toward the taking of appropriate action.

Glossary of specific terms used in this Recommendation

False declaration	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is required for submission in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.
False disclosure	refers to a misrepresentation of the value of currency or BNIs being transported, or a misrepresentation of other relevant data which is

© 2012-2019

Glossary of specific terms used in this Recommendation	
	asked for upon request in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.
Physical cross-border transportation	refers to any in-bound or out-bound physical transportation of currency or BNIs from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency or BNIs through containerised cargo or (3) the mailing of currency or BNIs by a natural or legal person.
Related to terrorist financing or money laundering	when used to describe currency or BNIs, refers to currency or BNIs that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; or (ii) laundered, proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

COMMISSION OF INQUIRY INTO STATE CAPTURE

INTERPRETIVE NOTE TO RECOMMENDATION 38 (MUTUAL LEGAL ASSISTANCE: FREEZING AND CONFISCATION)

1. Countries should consider establishing an asset forfeiture fund into which all, or a portion of, confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes. Countries should take such measures as may be necessary to enable them to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions.

2. With regard to requests for cooperation made on the basis of non-conviction based confiscation proceedings, countries need not have the authority to act on the basis of all such requests, but should be able to do so, at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

INTERPRETIVE NOTE TO RECOMMENDATION 40 (OTHER FORMS OF INTERNATIONAL COOPERATION)

A. PRINCIPLES APPLICABLE TO ALL FORMS OF INTERNATIONAL COOPERATION

Obligations on requesting authorities

1. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained.

Unduly restrictive measures

2. Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:

   (a) the request is also considered to involve fiscal matters; and/or

   (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or

   (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

   (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

Safeguards on information exchanged

3. Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties, or any use of this information for administrative, investigative, prosecutorial or judicial purposes, beyond those originally approved, should be subject to prior authorisation by the requested competent authority.

4. Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry[52], consistent with both parties' obligations concerning privacy and data protection. At a minimum, competent authorities should protect exchanged information in the same manner as they would protect similar information received from domestic sources. Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in the manner authorised. Exchange of

[52] Information may be disclosed if such disclosure is required to carry out the request for cooperation.

information should take place in a secure way, and through reliable channels or mechanisms. Requested competent authorities may, as appropriate, refuse to provide information if the requesting competent authority cannot protect the information effectively.

Power to search for information

5. Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically.

B. PRINCIPLES APPLICABLE TO SPECIFIC FORMS OF INTERNATIONAL COOPERATION

6. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.

Exchange of information between FIUs

7. FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.

8. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

9. FIUs should have the power to exchange:

   (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and

   (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.

Exchange of information between financial supervisors[53]

10. Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes.

---

[53] This refers to financial supervisors which are competent authorities.

© 2012-2019

11. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group:

    (a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors.

    (b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness.

    (c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information.

12. Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

13. Any dissemination of information exchanged or use of that information for supervisory and non- supervisory purposes, should be subject to prior authorisation by the requested financial supervisor, unless the requesting financial supervisor is under a legal obligation to disclose or report the information. In such cases, at a minimum, the requesting financial supervisor should promptly inform the requested authority of this obligation. The prior authorisation includes any deemed prior authorisation under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding issued by a core principles standard-setter applied to information exchanged under a Memorandum of Understanding or the Multi-lateral Memorandum of Understanding.

Exchange of information between law enforcement authorities

14. Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime.

15. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority.

16. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or

multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.

Exchange of information between non-counterparts

17. Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

18. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.

© 2012-2019

LEGAL BASIS OF REQUIREMENTS ON FINANCIAL INSTITUTIONS AND DNFBPS

1. All requirements for financial institutions or DNFBPs should be introduced either (a) in law (see the specific requirements in Recommendations 10, 11 and 20 in this regard), or (b) for all other cases, in law or enforceable means (the country has discretion).

2. In Recommendations 10, 11 and 20, the term "*law*" refers to any legislation issued or approved through a Parliamentary process or other equivalent means provided for under the country's constitutional framework, which imposes mandatory requirements with sanctions for non-compliance. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35). The notion of law also encompasses judicial decisions that impose relevant requirements, and which are binding and authoritative in all parts of the country.

3. The term "*Enforceable means*" refers to regulations, guidelines, instructions or other documents or mechanisms that set out enforceable AML/CFT requirements in mandatory language with sanctions for non-compliance, and which are issued or approved by a competent authority. The sanctions for non-compliance should be effective, proportionate and dissuasive (see Recommendation 35).

4. In considering whether a document or mechanism has requirements that amount to *enforceable means*, the following factors should be taken into account:

   (a) There must be a document or mechanism that sets out or underpins requirements addressing the issues in the FATF Recommendations, and providing clearly stated requirements which are understood as such. For example:

      (i) if particular measures use the word *shall* or *must*, this should be considered mandatory;

      (ii) if they use *should*, this could be mandatory if both the regulator and the regulated institutions demonstrate that the actions are directly or indirectly required and are being implemented; language such as measures *are encouraged*, *are recommended* or institutions *should consider* is less likely to be regarded as mandatory. In any case where weaker language is used, there is a presumption that the language is not mandatory (unless the country can demonstrate otherwise).

   (b) The document/mechanism must be issued or approved by a competent authority.

   (c) There must be sanctions for non-compliance (sanctions need not be in the same document that imposes or underpins the requirement, and can be in another document, provided that there are clear links between the requirement and the available sanctions), which should be effective, proportionate and dissuasive. This involves consideration of the following issues:

      (i) there should be an adequate range of effective, proportionate and dissuasive sanctions available if persons fail to comply with their obligations;

(ii) the sanctions should be directly or indirectly applicable for a failure to comply with an AML/CFT requirement. If non-compliance with an AML/CFT requirement does not have a sanction directly attached to it, then the use of sanctions for violation of broader requirements, such as not having proper systems and controls or not operating in a safe and sound manner, is satisfactory provided that, at a minimum, a failure to meet one or more AML/CFT requirements could be (and has been as appropriate) adequately sanctioned without a need to prove additional prudential failures unrelated to AML/CFT; and

(iii) whether there is satisfactory evidence that effective, proportionate and dissuasive sanctions have been applied in practice.

5. In all cases it should be apparent that financial institutions and DNFBPs understand that sanctions would be applied for non-compliance and what those sanctions could be.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

GENERAL GLOSSARY

Terms	Definitions
Accounts	References to "accounts" should be read as including other similar business relationships between financial institutions and their customers.
Accurate	Please refer to the IN to Recommendation 16.
Agent	For the purposes of Recommendations 14 and 16, *agent* means any natural or legal person providing MVTS on behalf of an MVTS provider, whether by contract with or under the direction of the MVTS provider.
Appropriate authorities	Please refer to the IN to Recommendation 8.
Associate NPOs	Please refer to the IN to Recommendation 8.
Batch transfer	Please refer to the IN to Recommendation 16.
Bearer negotiable instruments	*Bearer negotiable instruments (BNIs)* includes monetary instruments in bearer form such as: traveller's cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.
Bearer shares	*Bearer shares* refers to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
Beneficial owner	*Beneficial owner* refers to the natural person(s) who ultimately[54] owns or controls a customer[55] and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiaries	Please refer to the IN to Recommendation 8.
Beneficiary	The meaning of the term *beneficiary* in the FATF Recommendations depends on the context: ■ In trust law, a beneficiary is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts (other than charitable or

[54] Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

[55] This definition should also apply to beneficial owner of a beneficiary under a life or other investment linked insurance policy.

Terms	Definitions
	statutory permitted non-charitable trusts) are required to have ascertainable beneficiaries. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust perpetuity period which is usually referred to in the trust deed as the trust period. ■ In the context of life insurance or another investment linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy. Please also refer to the Interpretive Notes to Recommendation 16.
Beneficiary Financial Institution	Please refer to the IN to Recommendation 16.
Competent authorities	*Competent authorities* refers to all public authorities[56] with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency & BNIs; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as a competent authorities.
Confiscation	The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or

[56] This includes financial supervisors established as independent non-governmental authorities with statutory powers.

© 2012-2019

Terms	Definitions
	forfeited property is determined to have been derived from or intended for use in a violation of the law.
Core Principles	*Core Principles* refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.
Correspondent banking	*Correspondent banking* is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.
Country	All references in the FATF Recommendations to *country* or *countries* apply equally to territories or jurisdictions.
Cover Payment	Please refer to the IN. to Recommendation 16.
Criminal activity	*Criminal activity* refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in the country; or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3.
Cross-border Wire Transfer	Please refer to the IN to Recommendation 16.
Currency	*Currency* refers to banknotes and coins that are in circulation as a medium of exchange.
Designated categories of offences	*Designated categories of offences* means: ■ participation in an organised criminal group and racketeering; ■ terrorism, including terrorist financing; ■ trafficking in human beings and migrant smuggling; ■ sexual exploitation, including sexual exploitation of children; ■ illicit trafficking in narcotic drugs and psychotropic substances; ■ illicit arms trafficking; ■ illicit trafficking in stolen and other goods;

Terms	Definitions
	■ corruption and bribery; ■ fraud; ■ counterfeiting currency; ■ counterfeiting and piracy of products; ■ environmental crime; ■ murder, grievous bodily injury; ■ kidnapping, illegal restraint and hostage-taking; ■ robbery or theft; ■ smuggling; (including in relation to customs and excise duties and taxes); ■ tax crimes (related to direct taxes and indirect taxes); ■ extortion; ■ forgery; ■ piracy; and ■ insider trading and market manipulation. When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.
Designated non-financial businesses and professions	*Designated non-financial businesses and professions* means: a) Casinos[57] b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses,

[57] References to *Casinos* throughout the FATF Standards include internet- and ship-based casinos.

© 2012-2019

Terms	Definitions
	nor to professionals working for government agencies, who may already be subject to AML/CFT measures. f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: ■ acting as a formation agent of legal persons; ■ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; ■ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; ■ acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; ■ acting as (or arranging for another person to act as) a nominee shareholder for another person.
Designated person or entity	The term designated person or entity refers to: (i) individual, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1267 (1999) (the 1267 Committee), as being individuals associated with Al-Qaida, or entities and other groups and undertakings associated with Al-Qaida; (ii) individuals, groups, undertakings and entities designated by the Committee of the Security Council established pursuant to resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan, or entities and other groups and undertakings associated with the Taliban; (iii) any natural or legal person or entity designated by jurisdictions or a supra-national jurisdiction pursuant to Security Council resolution 1373 (2001); (iv) any individual, natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council

Terms	Definitions
	resolution 1718 (2006) and any future successor resolutions by the Security Council in annexes to the relevant resolutions, or by the Security Council Committee established pursuant to resolution 1718 (2006) (the 1718 Sanctions Committee) pursuant to Security Council resolution 1718 (2006); and (v) any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to Security Council resolution 2231 (2015) and any future successor resolutions by the Security Council.
Designation	The term *designation* refers to the identification of a person[58], individual or entity that is subject to targeted financial sanctions pursuant to: ■ United Nations Security Council resolution 1267 (1999) and its successor resolutions; ■ Security Council resolution 1373 (2001), including the determination that the relevant sanctions will be applied to the person or entity and the public communication of that determination; ■ Security Council resolution 1718 (2006) and any future successor resolutions; ■ Security Council resolution 2231 (2015) and any future successor resolutions; and ■ any future Security Council resolutions which impose targeted financial sanctions in the context of the financing of proliferation of weapons of mass destruction. As far as Security Council resolution 2231 (2015) and any future successor resolutions are concerned, references to "designations" apply equally to "listing".
Domestic Wire Transfer	Please refer to the IN to Recommendation 16.
Enforceable means	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Ex Parte	The term *ex parte* means proceeding without prior notification and participation of the affected party.
Express trust	*Express trust* refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts

58 Natural or legal.

© 2012-2019

Terms	Definitions
	which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).
False declaration	Please refer to the IN to Recommendation 32.
False disclosure	Please refer to the IN to Recommendation 32.
Financial group	*Financial group* means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Financial institutions	*Financial institutions* means any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public.[59] 2. Lending.[60] 3. Financial leasing.[61] 4. Money or value transfer services.[62] 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments; (d) transferable securities; (e) commodity futures trading.

59 This also captures private banking.

60 This includes *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).

61 This does not extend to financial leasing arrangements in relation to consumer products.

62 It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretive Note to Recommendation 16.

Terms	Definitions
	8. Participation in securities issues and the provision of financial services related to such issues. 9. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance[63]. 13. Money and currency changing.
Foreign counterparts	Foreign counterparts refers to foreign competent authorities that exercise similar responsibilities and functions in relation to the cooperation which is sought, even where such foreign competent authorities have a different nature or status (e.g. depending on the country, AML/CFT supervision of certain financial sectors may be performed by a supervisor that also has prudential supervisory responsibilities or by a supervisory unit of the FIU).
Freeze	In the context of confiscation and provisional measures (e.g., Recommendations 4, 32 and 38), the term freeze means to prohibit the transfer, conversion, disposition or movement of any property, equipment or other instrumentalities on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism, or until a forfeiture or confiscation determination is made by a competent authority. For the purposes of Recommendations 6 and 7 on the implementation of targeted financial sanctions, the term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons or entities on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court. In all cases, the frozen property, equipment, instrumentalities, funds or other assets remain the property of the natural or legal person(s) that held an interest in them at the time of the freezing and may continue to be administered by third parties, or through other arrangements established by such natural or legal person(s) prior to the initiation of an action under a freezing mechanism, or in accordance with other national provisions. As part of the implementation of a freeze, countries may decide to take control of the property, equipment, instrumentalities, or funds or other assets as a means to protect against flight.

[63] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

© 2012-2019

Terms	Definitions
Fundamental principles of domestic law	This refers to the basic legal principles upon which national legal systems are based and which provide a framework within which national laws are made and powers are exercised. These fundamental principles are normally contained or expressed within a national Constitution or similar document, or through decisions of the highest level of court having the power to make binding interpretations or determinations of national law. Although it will vary from country to country, some examples of such fundamental principles include rights of due process, the presumption of innocence, and a person's right to effective protection by the courts.
Funds	The term *funds* refers to assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets.
Funds or other assets	The term *funds or other assets* means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.
Identification data	The term *identification data* refers to reliable, independent source documents, data or information.
Intermediary financial institution	Please refer to the IN to Recommendation 16.
International organisations	International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Co-operation in Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

Terms	Definitions
Law	Please refer to the Note on the Legal Basis of requirements on Financial Institutions and DNFBPs.
Legal arrangements	*Legal arrangements* refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso.
Legal persons	*Legal persons* refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.
Money laundering offence	References (except in Recommendation 3) to a *money laundering offence* refer not only to the primary offence or offences, but also to ancillary offences.
Money or value transfer service	*Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala*, *hundi*, and *fei-chen*.
Non-conviction based confiscation	*Non-conviction based confiscation* means confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required.
Non-profit organisations	Please refer to the IN to Recommendation 8.
Originator	Please refer to the IN to Recommendation 16.
Ordering financial institution	Please refer to the IN to Recommendation 16.
Payable-through accounts	Please refer to the IN to Recommendation 13.
Physical cross-border transportation	Please refer to the IN. to Recommendation 32.

© 2012-2019

Terms	Definitions
Politically Exposed Persons (PEPs)	*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Persons who are or have been entrusted with a prominent function by an international organisation* refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Proceeds	*Proceeds* refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	*Property* means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Qualifying wire transfers	Please refer to the IN to Recommendation 16.
Reasonable measures	The term *Reasonable Measures* means: appropriate measures which are commensurate with the money laundering or terrorist financing risks.
Related to terrorist financing or money laundering	Please refer to the IN. to Recommendation 32.
Required	Please refer to the IN to Recommendation 16.
Risk	All references to *risk* refer to the risk of money laundering and/or terrorist financing. This term should be read in conjunction with the Interpretive Note to Recommendation 1.
Satisfied	Where reference is made to a financial institution being *satisfied* as to a matter, that institution must be able to justify its assessment to competent authorities.
Seize	The term *seize* means to prohibit the transfer, conversion, disposition or movement of property on the basis of an action initiated by a competent

Terms	Definitions
	authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified property. The seized property remains the property of the natural or legal person(s) that holds an interest in the specified property at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized property.
Self-regulatory body (SRB)	A SRB is a body that represents a profession (e.g. lawyers, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practise in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practising the profession.
Serial Payment	Please refer to the IN. to Recommendation 16.
Settlor	*Settlors* are natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.
Shell bank	*Shell bank* means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. *Physical presence* means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Should	For the purposes of assessing compliance with the FATF Recommendations, the word *should* has the same meaning as *must.*
Straight-through processing	Please refer to the IN. to Recommendation 16.
Supervisors	*Supervisors* refers to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial institutions ("*financial supervisors*" [64]) and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

[64] Including Core Principles supervisors who carry out supervisory functions that are related to the implementation of the FATF Recommendations.

© 2012-2019

Terms	Definitions
Targeted financial sanctions	The term *targeted financial sanctions* means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
Terrorist	The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A *terrorist act* includes: (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	*Terrorist financing* is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist financing abuse	Please refer to the IN to Recommendation 8.
Terrorist financing offence	References (except in Recommendation 4) to a *terrorist financing offence* refer not only to the primary offence or offences, but also to ancillary offences.

Terms	Definitions
Terrorist organisation	The term *terrorist organisation* refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Third parties	For the purposes of Recommendations 6 and 7, the term *third parties* includes, but is not limited to, financial institutions and DNFBPs. Please also refer to the IN to Recommendation 17.
Trustee	The terms *trust* and *trustee* should be understood as described in and consistent with Article 2 of the *Hague Convention on the law applicable to trusts and their recognition*[65]. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family).
Unique transaction reference number	Please refer to the IN. to Recommendation 16.
Virtual Asset	A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

[65] Article 2 of the Hague Convention reads as follows:

For the purposes of this Convention, the term "trust" refers to the legal relationships created – inter-vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose.

A trust has the following characteristics -

a) the assets constitute a separate fund and are not a part of the trustee's own estate;

b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee;

c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.

The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust.

© 2012-2019

Terms	Definitions
Virtual Asset Service Providers	Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer[66] of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
Without delay	The phrase without delay means, ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of weapons of mass destruction, and the need for global, concerted action to interdict and disrupt their flow swiftly.

[66] In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

TABLE OF ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for *Combating the financing of terrorism*)
BNI	Bearer-Negotiable Instrument
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
IN	Interpretive Note
ML	Money Laundering
MVTS	Money or Value Transfer Service(s)
NPO	Non-Profit Organisation
Palermo Convention	The United Nations Convention against Transnational Organized Crime 2000
PEP	Politically Exposed Person
R.	Recommendation
RBA	Risk-Based Approach
SR.	Special Recommendation
SRB	Self-Regulatory Bodies
STR	Suspicious Transaction Report
TCSP	Trust and Company Service Provider
Terrorist Financing Convention	The International Convention for the Suppression of the Financing of Terrorism 1999
UN	United Nations
Vienna Convention	The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

© 2012-2019

ANNEX I: FATF GUIDANCE DOCUMENTS

The FATF has published a large body of Guidance and Best Practices papers which can be found at: www.fatf-gafi.org/documents/guidance/.

COMMISSION OF INQUIRY INTO STATE CAPTURE

ANNEX II: INFORMATION ON UPDATES MADE TO THE FATF RECOMMENDATIONS

The following amendments have been made to the FATF Recommendations since the text was adopted in February 2012.

Date	Type of amendments	Sections subject to amendments
Feb 2013	Alignment of the Standards between R.37 and R.40	■ R.37(d) – page 27 Insertion of the reference that DNFBP secrecy or confidentiality laws should not affect the provision of mutual legal assistance, except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies.
Oct 2015	Revision of the Interpretive Note to R. 5 to address the foreign terrorist fighters threat	■ INR.5 (B.3) – page 37 Insertion of B.3 to incorporate the relevant element of UNSCR 2178 which addresses the threat posed by foreign terrorist fighters. This clarifies that Recommendation 5 requires countries to criminalise financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. Existing B.3-11 became B.4-12.
Jun 2016	Revision of R. 8 and the Interpretive Note to R. 8	■ R.8 and INR.8 – pages 13 and 54-59 Revision of the standard on non-profit organisation (NPO) to clarify the subset of NPOs which should be made subject to supervision and monitoring. This brings INR.8 into line with the FATF Typologies Report on Risk of Terrorist Abuse of NPOs (June 2014) and the FATF Best Practices on Combatting the Abuse of NPOs (June 2015) which clarify that not all NPOs are high risk and intended to be addressed by R.8, and better align the implementation of R.8/INR.8 with the risk-based approach.

© 2012-2019

Date	Type of amendments	Sections subject to amendments
Oct 2016	Revision of the Interpretive Note to R. 5 and the Glossary definition of 'Funds or other assets'	■ INR. 5 and Glossary – pages 37 and 121 Revision of the INR.5 to replace "*funds*" with "*funds or other assets*" throughout INR.5, in order to have the same scope as R.6. Revision of the Glossary definition of "*funds or other assets*" by adding references to oil and other natural resources, and to other assets which may potentially be used to obtain funds.
Jun 2017	Revision of the Interpretive Note to R.7 and the Glossary definitions of "Designated person or entity", "Designation" and "Without delay"	■ INR. 7 and Glossary – pages 45-51, 114-115 and 123 Revision of the INR.7 and consequential revisions of the Glossary definitions of *"Designated person or entity"*, *"Designation"* and *"Without delay"* to bring the text in line with the requirements of recent United Nations Security Council Resolutions and to clarify the implementation of targeted financial sanctions relating to proliferation financing.
Nov 2017	Revision of the Interpretive Note to Recommendation 18	■ INR.18 – page 77 Revision of INR.18 to clarify the requirements on sharing of information related to unusual or suspicious transactions within financial groups. It also includes providing this information to branches and subsidiaries when necessary for AML/CFT risk management.
Nov 2017	Revision of Recommendation 21	■ R. 21 – page 17 Revision of R. 21 to clarify the interaction of these requirements with tipping-off provisions.
Feb 2018	Revision of Recommendation 2	■ R. 2 – page 9 Revision of R. 2 to ensure compatibility of AML/CFT requirements and data protection and privacy rules, and to promote domestic inter-agency information sharing among competent authorities.

Date	Type of amendments	Sections subject to amendments
Oct 2018	Revision of Recommendation 15 and addition of two new definitions in the Glossary	■ R. 15 and Glossary – pages 15 and 126-127 Revision of R.15 and addition of new definitions "virtual asset" and "virtual asset service provider" in order to clarify how AML/CFT requirements apply in the context of virtual assets.
June 2019	Addition of Interpretive Note to R. 15	■ INR. 15 – page 70-71 Insertion of a new interpretive note that sets out the application of the FATF Standards to virtual asset activities and service providers.

COMMISSION OF INQUIRY INTO STATE CAPTURE

© 2012-2019

FATF

www.fatf-gafi.org

COMMISSION OF INQUIRY INTO STATE CAPTURE

Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001)

(South African Legislation)

South African Reserve Bank Act, 1989 (Act No. 90 of 1989)
Regulations Relating to the South African Reserve Bank

(South African Legislation)

COMMISSION OF INQUIRY INTO STATE CAPTURE

CORRUPTION WATCH

Official website for the South African Corruption Watch

https://www.corruptionwatch.org.za/

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-406

Law Commission
Reforming the law

Anti-Money Laundering: the SARs Regime
Consultation Paper

COMMISSION OF INQUIRY INTO STATE CAPTURE

Consultation Paper No 236

PH-407

Law Commission
Reforming the law

Consultation Paper No 236

Anti-Money Laundering: the SARs Regime

Consultation Paper

20 July 2018

© Crown copyright 20 June 2018

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: mpsi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.lawcom.gov.uk/project/anti-money-laundering/.

THE LAW COMMISSION – HOW WE CONSULT

About the Law Commission: The Law Commission was set up by section 1 of the Law Commissions Act 1965 for the purpose of promoting the reform of the law. The Law Commissioners are: The Right Honourable Lord Justice Bean, Chair, Professor Nicholas Hopkins, Stephen Lewis, Professor David Ormerod QC and Nicholas Paines QC. The Chief Executive is Phillip Golding.

Topic of this consultation: This consultation paper seeks to obtain consultees' views on proposals to reform the law governing anti-money laundering.

Geographical scope: This consultation paper applies to the law of England and Wales.

Availability of materials: This consultation paper is available on our website at https://www.lawcom.gov.uk/project/anti-money-laundering/

Duration of the consultation: We invite responses from 20 July 2018 until 5 October 2018.

Comments may be sent:

By email: anti-money-laundering@lawcommission.gov.uk.

By post: Criminal Team, 1st Floor, Tower, Post Point 1.54, 52 Queen Anne's Gate, London SW1H 9AG (access via 102 Petty France)

By telephone: 020 3334 0200

If you send your comments by post, it would be helpful if, whenever possible, you could also send them electronically.

After the consultation: In the light of the responses we receive, we will decide on our final recommendations and present them to Government.

Consultation principles: The Law Commission follows the Consultation Principles set out by the Cabinet Office, which provide guidance on type and scale of consultation, duration, timing, accessibility and transparency. The Principles are available on the Cabinet Office website at: https://www.gov.uk/government/publications/consultation-principles-guidance.

Information provided to the Law Commission: We may publish or disclose information you provide us in response to Law Commission papers, including personal information. For example, we may publish an extract of your response in Law Commission publications, or publish the response in its entirety. We may also share any responses received with Government. Additionally, we may be required to disclose the information, such as in accordance with the Freedom of Information Act 2000. If you want information that you provide to be treated as confidential please contact us first, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic disclaimer generated by your IT system will not be regarded as binding on the Law Commission. The Law Commission

will process your personal data in accordance with the General Data Protection Regulations, which came into force in May 2018.

Any concerns about the contents of this Privacy Notice can be directed to: general.enquiries@lawcommission.gov.uk

COMMISSION OF INQUIRY INTO STATE CAPTURE

Contents

	page
GLOSSARY	1
CHAPTER 1: INTRODUCTION	**3**
The project	3
Background	4
The current law	5
Overview	5
The consent regime	7
The consultation paper	11
The purpose of the paper	11
Scheme of the paper	12
Acknowledgments	17
CHAPTER 2: MONEY LAUNDERING	**19**
Transaction monitoring: the pre-suspicion stage	19
The suspicious activity reporting process	21
Types of disclosure	21
The seven-day notice period	22
The moratorium period	24
The failure to disclose offences	26
Failure to disclose by those working within the regulated sector	27
Failure to disclose by nominated officers working in the regulated sector	27
Failure to disclose by other nominated officers	28
Exemptions from the failure to disclose offences	29
Issues arising from the failure to disclose offences	31
The money laundering offences	32
Penalty	33
Key concepts	33
Exemptions or defences to the principal money laundering offences	35
The five common exemptions	36
The adequate consideration exemption	37
The authorised disclosure exemption	37
Tipping off	40
Exemptions from tipping off	40
Issues arising from tipping off	41
Information sharing	43
Joint Money Laundering Intelligence Taskforce (JMLIT)	43

Information sharing under the Criminal Finances Act 2017 44

Regulating businesses and professionals 45
The Money Laundering Regulations 2017 45
Supervisory authorities 46
OPBAS 47

CHAPTER 3: TERRORISM FINANCING 49

Background 49

The current law 50
Overview of the Terrorism Act 2000 50
Disclosure of information 51
The suspicious activity reporting process: terrorism 51
Terrorism offences 53
Issues with terrorism financing SARs 57

CHAPTER 4: MEASURING EFFECTIVENESS 59
Causes of the large volume of reports 62

CHAPTER 5: THE "ALL CRIMES" APPROACH 65
"Technical" breaches 66
"Serious crimes" rather than "all crimes" 67
Consultation Question 1. 69

CHAPTER 6: THE MEANING OF SUSPICION 71

The concept of suspicion 71
Concerns about suspicion 72
Why are the thresholds set at the level of suspicion? 74

Suspicion in criminal law 76
The ordinary meaning of suspicion 76
Suspicion in the hierarchy of fault 77
Suspicion based tests in the investigative context 83
Suspicion-based tests in the Proceeds of Crime Act 2002 87

CHAPTER 7: THE APPLICATION OF THE CONCEPT OF SUSPICION IN THE CONTEXT OF THE MONEY LAUNDERING OFFENCES 89

Case law on suspicion in the context of money laundering offences 89
Reasonable grounds for suspicion in the context of money laundering offences 91
Guidance on suspicion 93
Criticisms of the suspicion test in the context of money laundering offences 95
Challenges created by the suspicion test in the context of money laundering offences 96

CHAPTER 8: THE APPLICATION OF THE TEST OF SUSPICION IN THE CONTEXT OF THE DISCLOSURE OFFENCES **99**
The disclosure offences 99
The threshold of the offences 101
The implications of the current threshold: "suspects" or "has reasonable grounds for suspecting" 109

CHAPTER 9: THE CASE FOR REFORMING THE SUSPICION THRESHOLD **113**
Should suspicion be defined? 113
Consultation Question 2. 114
Would guidance improve the application of suspicion by the reporting sector? 114
Consultation Question 3. 116
Prescribed form 116
Consultation Question 4. 116
Consultation Question 5. 116
The alternative threshold: *Saik* "reasonable grounds to suspect" 117
Adopting a test of reasonable grounds for suspicion in relation to required disclosures 119
Consultation Question 6. 127
Consultation Question 7. 127
Consultation Question 8. 127
Consultation Question 9. 128

CHAPTER 10: CRIMINAL PROPERTY AND MIXED FUNDS **129**
Overview 129
Fungibility 131
Mixed funds 132
Other approaches in the Proceeds of Crime Act 2002 135
A way forward on the issue of mixed funds 136
Consultation Question 10. 138
Consultation Question 11. 138

CHAPTER 11: THE SCOPE OF REPORTING **141**
Consultation Question 12. 142
Low value transactions 142
Consultation Question 13. 144
Consultation Question 14. 144
Internal movement of funds 144
Consultation Question 15. 145
Duplicate reporting obligations 145
Consultation Question 16. 146
Consultation Question 17. 146
Information in the public domain 146
Consultation Question 18. 147
Property transactions within the UK 147
Consultation Question 19. 148

Consultation Question 20. 148
Multiple transactions and related accounts 148
Consultation Question 21. 148
Repayment to victoms of fraud 149
Consultation Question 22. 149
Historical crime 149
Consultation Question 23. 149
Consultation Question 24. 149
No UK nexus 149
Consultation Question 25. 150
Disclosures instigated by law enforcement agencies 150
Consultation Question 26. 150

CHAPTER 12: THE MEANING OF CONSENT 153
Problems with the term "consent" 154
Current approach 155
Alternative terms 156
Options for reform 157
Consultation Question 27. 158
Consultation Question 28. 158

CHAPTER 13: INFORMATION SHARING 159
The need for effective information sharing 159
Existing provisions to obtain and share information 159
Data protection provisions 161
Reform options 164
Stakeholders' views 164
Pre-suspicion data sharing 165
Consultation Question 29. 170
Consultation Question 30. 170
Improving information sharing partnerships 171
Consutlation Question 31 174
Consultation Question 32 174
Consutlation Question 33 174

CHAPTER 14: ENHANCING THE CONSENT REGIME AND ALTERNATIVE APPROACHES 175
Overview 175
Alternative models to seeking consent 175
Removing the authorised disclosure exemption 175
Consultation Question 34. 179
Alternative approaches to the consent regime 179
Thematic reporting 179
Consultation Question 35. 184
Consultation Question 36. 184
Corporate criminal liability 184
Consultation Question 37. 186
Consultation Question 38. 187

CHAPTER 15: CONSULTATION QUESTIONS **188**

APPENDIX 1: LIST OF ACRONYMS **199**

APPENDIX 2: CURRENT END USERS WITH 'DIRECT' ACCESS **200**

APPENDIX 3: GOVERNMENT DEPARTMENTS, ORGANISATIONS AND INDIVIDUALS CONSULTED **203**

APPENDIX 4: THE REGULATED SECTOR **207**

COMMISSION OF INQUIRY INTO STATE CAPTURE

COMMISSION OF INQUIRY INTO STATE CAPTURE

Glossary

Beneficial Owner - Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.[1]

Debanking - The practice of withdrawing banking facilities from a customer due to the perceived risk they present to the bank.

DNFBP - Designated non-financial businesses and professions are: casinos; real estate agents; dealers in previous metals; dealers in precious stones; lawyers, notaries, other independent legal professionals and accountants; and trust and company service providers.

FATF - Financial Action Task Force is an intergovernmental body whose objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

Mandate - A service contract between a customer and their bank which gives the bank authority to act on the customer's behalf.

Money Service Businesses - undertaking which by way of business operates a currency exchange office, transmits money (or any representation of monetary value) by any means or cashes cheques which are made payable to customers.[2]

Legal persons - Legal persons refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

PEP - Politically exposed persons are individuals who are or have been entrusted with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. PEPs may be foreign or domestic.

SAR - Suspicious Activity Reports are an electronic or paper document in which the reporter discloses their suspicions of money laundering in accordance with their obligations under sections 330-332 and 338 of the Proceeds of Crime Act 2002. These reports are lodged

---

1 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf at page 111.

2 'The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (UK)' [MLRs 2017], Chapter 3.

with the National Crime Agency. In other jurisdictions the equivalent to SARs are also known as suspicious transaction reports (STRs) or suspicious matter reports (SMRs).

Shell bank - Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

Terrorist Financing - Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.

COMMISSION OF INQUIRY INTO STATE CAPTURE

Chapter 1: Introduction

THE PROJECT

1.1 In 2017, the Law Commission agreed with the Home Office to review and make proposals for reform of limited aspects of the anti-money laundering regime in Part 7 of the Proceeds of Crime Act 2002 ("POCA") and of the counter-terrorism financing regime in Part 3 of the Terrorism Act 2000. This followed a discussion of ideas for inclusion in the Law Commission's thirteenth Programme of Law Reform. The primary purpose of the review is to improve the prevention, detection and prosecution of money laundering and terrorism financing in the United Kingdom.[1]

1.2 We agreed the following terms of reference with the Home Office:

(1) The review will cover the reporting of suspicious activity in order to seek a defence against money laundering or terrorist financing offences in relation to both regimes. Specifically, the review will focus on the consent provisions in sections 327 to 329 and sections 335, 336 and 338 of POCA, and in sections 21 to 21ZC of the Terrorism Act 2000.

(2) The review will also consider the interaction of the consent provisions with the disclosure offences in sections 330 to 333A of POCA and sections 19, 21A and 21D of the Terrorism Act 2000.

(3) To achieve that purpose, the review will analyse the functions of, and benefits and problems arising from, the consent regime, including:

(a) the defence provided by the consent regime to the money laundering and terrorism financing offences;

(b) the ability of law enforcement agencies to suspend suspicious transactions and thus investigate money laundering and restrain assets;

(c) the ability of law enforcement agencies to investigate, and prosecutors to secure convictions, as a consequence of the wide scope of the money laundering and terrorist financing offences;

(d) the abuse of the automatic defence to money laundering and terrorism financing offences provided by the consent provisions;

(e) the underlying causes of the defensive over-reporting of suspicious transactions under the consent and disclosure provisions;

(f) the burden placed by the consent provisions and disclosure provisions on entities under duties to report suspicious activity; and

[1] It should be noted throughout this paper that the Law Commission's remit covers England and Wales only.

(g) the impact of the suspension of transactions under the consent provisions on reporting entities and entities that are the subject of reporting.

(4) The review will then produce reform options that address these issues. In doing so, the review will take into consideration the Fourth Anti-Money Laundering Directive ("4AMLD")[2] and the recommendations of the Financial Action Task Force ("FATF"), as well as the effect of new legislation or directives, such as the Criminal Finances Act 2017, the Fifth Anti-Money Laundering Directive ("5AMLD")[3], the Payment Services Directive 2, and the General Data Protection Regulation.[4]

(5) The review will also gather ideas for wider reform which may go beyond the focused terms of reference noted above. These will be intended to provide a basis for future development of the anti-money laundering and counter terrorism financing regimes.

1.3 Work commenced on the project in February 2018. Since the project began, many stakeholders have agreed that the review is timely. The majority of stakeholders have endorsed the view that there are practical problems in the operation of the reporting regime which have a tangible impact on the private sector, law enforcement agencies and the wider public.

BACKGROUND

1.4 It is not possible to value accurately the annual turnover of the proceeds of crime committed nationally or worldwide. Most experts agree that no reliable estimates exist. There have been attempts to place a value on domestic crime over the years. In 2005, HMRC estimated that the annual proceeds of crime in the UK were between £19 billion and £48 billion. They concluded that £25 billion was the best estimate for the amount of money laundered per annum at that time.[5] This represented a small fraction of the overall value of transactions conducted by UK-based banks at the same time, estimated at approximately £5,500 billion per annum.[6]

---

2 Directive (EU) 2015/849 of 20 May 2015 the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

3 Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU http://data.consilium.europa.eu/doc/document/PE-72-2017-INIT/en/pdf (accessed on 23 May 2018).

4 Regulation (EU) 2016/679 of the European Parliament and of the Council amending Directive 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

5 Corporation of London, *Anti-Money Laundering Requirements: Costs, Benefits and Perceptions* (June 2005), p 15.

6 Corporation of London, *Anti-Money Laundering Requirements: Costs, Benefits and Perceptions* (June 2005), p 16.

1.5 The United Nations Office for Drugs and Crime[7] estimated the annual value of "all criminal proceeds" for 2009 at approximately US$2.1 trillion (or an average of 3.6% of global gross domestic product ("GDP") (2.3% to 5.5%)). The amount estimated to be available for laundering in the same year through the financial system amounted to some US$1.6 trillion (equivalent to an average of 2.7% of global GDP (2.1% to 4%)). Given the difficulty in arriving at estimates, academics have drawn attention to evidence of data being repeated and recycled across official reports.[8]

1.6 One of the difficulties inherent in estimating the value of proceeds of crime is that many forms of criminal activity are cash intensive. Any offender who wants to spend or invest money obtained from their crimes without attracting the attention of law enforcement agencies will seek to disguise or hide the source of their funds. Whilst techniques vary,[9] it is generally agreed that money laundering is the processing of these criminal proceeds to disguise their illegal origin.

1.7 Given the difficulties in identifying criminal funds once they are within the financial system, intelligence from the private sector at the placement stage is crucial. The safety, convenience and legitimacy conveyed by a bank account means that the majority of people, including criminals, will conduct some of their financial affairs through large financial institutions. Banks are able to monitor unusual activity and provide information to the authorities within a legal framework set down by Part 7 of POCA.[10] In this way, they perform a vital law enforcement agencies function.

THE CURRENT LAW

Overview

1.8 The existing anti-money laundering and terrorism financing regime in the UK can be divided into four parts.

(1) POCA received Royal Assent on 24 July 2002. Part 7 was intended to replace and improve upon the preceding money laundering legislation. Part 7 created:

---

7 United Nations Office on Drugs and Crime (UNODC): '*Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes: Research Report*' (October 2011); key findings, cited in '*UK national risk assessment of money laundering and terrorist financing*' (HM Treasury and Home Office, October 2015); and EUROPOL '*Criminal Asset Recovery in the EU: Does crime still pay? Survey of statistical information 2010-2014*'; 2016, p.5. Estimates of worldwide turnover of organized crime, set out in Table 31, page 38, to the 2011 UNODC Report, is reproduced at Appendix A.

8 Duyne, P.C. van, Harvey J., & Gelemerova, L (2016), *'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality'* Chapter 10 in *'Illegal Entrepreneurship, Organized Crime and Social Control: Essays in Honour of Professor Dick Hobbs'* (ed) G. Antonopolous, Springer, Studies in Organized Crime 14.

9 A Kennedy, "Dead Fish across the Trail: Illustrations of Money Laundering Methods" (2005) *8 Journal of Money Laundering Control*, 306-315. For a review of current money laundering techniques, see also National Crime Agency, *National Strategic Assessment of Serious and Organised Crime* (2018), p 38 to 40.

10 The parallel regime under the Terrorism Act 2000 will also be considered in this paper.

(a) three offences of money laundering which apply to the proceeds of any criminal offence;[11]

(b) legal obligations to report suspected money laundering bolstered by criminal offences for failures to disclose;[12]

(c) a complementary "consent regime" of authorised disclosures which offer protection from criminal liability;[13] and

(d) a prohibition on warning the (alleged) money launderer that a report had been made to the authorities or an investigation had begun ("tipping off").[14]

(2) A parallel regime operates in relation to counter-terrorism financing and is contained in Part 2 of the Terrorism Act 2000. We will consider terrorism financing in detail in Chapter 3.

(3) Domestic anti-money laundering provisions have been supplemented by successive EU Directives on money laundering. These have been implemented by Regulation in the UK. 4AMLD was agreed in June 2015 and implemented in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("The Money Laundering Regulations 2017"). The Money Laundering Regulations 2017 create a system of regulatory obligations for businesses under the supervision of the Financial Conduct Authority and the relevant professional and regulatory bodies recognised within the Regulations. At the time of writing, the UK is negotiating its exit from the EU. It is unclear how this may impact on the UK's obligations under EU law in respect of anti-money laundering and counter terrorism financing. However, it is assumed for the purposes of this consultation paper that the drive to harmonise standards across states as far as possible is unlikely to change and that we will continue to comply with the terms of the 4AMLD for the foreseeable future.

(4) Whilst POCA and the 4AMLD form the foundation of the UK's anti-money laundering regime, domestic law must be considered in the context of agreed international standards. The UK is one of the founding members of FATF, an inter-governmental body established in 1989 to set standards in relation to combatting money laundering and terrorist financing. Its recommendations are recognised as the international standard for anti-money laundering regulation. The recommendations set out a framework of measures to be implemented by its members and monitored through a peer review process of mutual evaluation.[15]

---

11 Proceeds of Crime Act 2002, ss 327 to 329.

12 Proceeds of Crime Act 2002, ss 330 to 332.

13 Proceeds of Crime Act 2002, ss 327(2)(a), 328(2)(a), 329(2)(a).

14 Proceeds of Crime Act 2002, s 330A.

15 See FATF's website at http://www.fatf-gafi.org/. Mutual Evaluation Reports can be accessed at http://www.fatf-gafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate) (last visited on 24 April 2018).

The consent regime

Required and authorised disclosures

1.9 The consent regime refers to the process whereby an individual who suspects that they are dealing with the proceeds of crime can seek permission to complete a transaction by disclosing their suspicion to the UK Financial Intelligence Unit ("UKFIU") which is housed within the National Crime Agency ("NCA"). In order to understand how the consent regime operates, it is necessary to consider the types of disclosure that a bank or business might make when they suspect someone is engaged in money laundering or, for example, comes into possession of what they suspect may be the proceeds of crime.

1.10 There are two types of disclosure that a bank or business may make: "required disclosures" and "authorised disclosures." We will consider these disclosures in more detail in Chapter 2, but for present purposes, the important distinction is between whether the disclosure is required by law or whether the reporter wishes to protect themselves from a potential money laundering charge.

1.11 Required disclosures are triggered by one of the statutory duties to disclose under POCA, where a person knows, suspects or has reasonable grounds to know or suspect that a person is engaged in money laundering.[16] If they are not made, the person who ought to have reported is liable for prosecution for a criminal offence.

1.12 In contrast, authorised disclosures have a dual function: they both provide intelligence to the law enforcement agencies, and protect the discloser from relevant criminal liability. For example, a bank may become suspicious that funds in a customer's account are the proceeds of crime. If their customer asks the bank to make a payment in accordance with their mandate, disclosure is made to obtain consent to proceed with the transaction and bring the individual within a statutory exemption which effectively precludes any future money laundering charge against the reporter.[17]

1.13 Whilst both types of disclosure will be examined in detail in this paper, authorised disclosures and the consent exemption ("the consent regime") will be the principal focus.

Suspicious activity reports

1.14 Suspicious activity reports ("SARs") are the mechanism by which the private sector make disclosures in relation to money laundering and terrorism financing under POCA.[18] The SAR is the format in which the UKFIU receive information. The UKFIU facilitates the disclosure process by acting as the intermediary for intelligence between the private sector and law enforcement agencies. When a SAR is submitted, it is analysed and made available to law enforcement agencies who will investigate and decide whether to take further action. Because of the time it takes to conduct an investigation and intervene to preserve criminal assets, the scheme obliges the bank to

---

16 Proceeds of Crime Act 2002, ss 330, 331 and 332.

17 Proceeds of Crime Act 2002, ss 327(2), 328(2) and 329(2).

18 More specifically it is the regulated sector who are most heavily impacted by the SARs regime. The regulated sector is defined in Schedule 9 to the Proceeds of Crime Act 2002.

refrain from processing the transaction once a SAR is submitted. This time allows the NCA to take a fully informed decision on whether to consent to the transaction.

1.15 High quality SARs can be a vital source of intelligence.[19] They can provide evidence of money laundering in action. Furthermore, SARs are one of the primary methods of sharing information to produce intelligence for law enforcement agencies to investigate and prosecute crime more generally.[20] Identifying the proceeds of criminal activity can establish an investigative trail leading law enforcement agencies back to the original criminal activity. A SAR may trigger an investigation or provide a useful resource for an investigation that is already ongoing.

1.16 Multiple SARs on the same subject can trigger investigations into a new target. For example, if a bank and a law firm are both working on the same transaction and each reports suspicious activity, this provides a richer intelligence picture to the authorities. Information from these reports can lead to the recovery of the proceeds of crime by assisting in restraint orders, confiscation orders and cash seizures although the quality of the intelligence gathered depends, in part, on the quality of the information provided in the SAR. Inferior quality SARs are more time intensive to process, can contribute to delay in the system and may ultimately remain of little value to law enforcement agencies.

Cost to the economy

1.17 The reporting regime impacts on the legitimate economy in two ways. First, there is a considerable cost to businesses in ensuring compliance with their reporting obligations. Secondly, there is a cost to the taxpayer in resourcing the receipt and analysis of reports to assist law enforcement agencies. It is worth considering whether the cost of the regime is proportionate and whether it is as efficient as it could be.

1.18 The level of burden placed upon the reporter depends upon whether they are operating within or outside the regulated sector. The legislation brings a broad range of businesses within the scope of the regulated sector. For example, it includes financial institutions, those providing accountancy services, tax advisory or investment services, those participating in financial or real property transactions (including legal professionals), insolvency practitioners, high value dealers and casinos amongst others.[21]

1.19 The largest reporting sector is banking. Between October 2015 and March 2017, banks accounted for 82.85% of the 634,113 SARs submitted to the UKFIU.[22] Adding together the percentages of SARs from all other types of credit or financial institutions brings this figure to 95.78%. Overwhelmingly, the financial sector bears the greatest burden.[23] This is understandable when we consider the volume of transactions processed by the

---

19 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017), p 5.

20 HM Treasury and Home Office, *National risk assessment of money laundering and terrorist financing*, (October 2017).

21 Proceeds of Crime Act 2002, s 330(12) and Sch 9.

22 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017), fig i.

23 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017), pp 12 to 13.

financial sector. The large retail banks are conducting transactions on an industrial scale. One of the largest reporting banks receives an average 3300 automated alerts per month highlighting unusual activity. However, this can fluctuate and has been known to rise to over 7,000 alerts per month. In addition, a further 14,200 internal reports of potentially suspicious activity from staff will be submitted each month.

1.20 It has been estimated that the cost of the anti-money laundering system to a large reporting bank is in the region of tens of millions of pounds per year.[24] The British Bankers' Association (now UK Finance) estimated that its members are spending at least £5 billion annually on core financial crime compliance, including enhanced systems and controls and recruitment of staff.[25] High costs attributed to anti-money laundering requirements may reduce confidence in the efficiency of the system.[26] It is also essential to identify whether the right balance between reputation and competitiveness has been struck in the UK. Anti-money laundering regulation is essential to ensuring that the integrity of the UK's financial sector. However, the UK's competitive position has the potential to be undermined by unnecessary regulation or regulation which fails to produce verifiable results.[27]

1.21 Whilst the financial sector is the largest reporting sector, there are significant compliance costs for every sector with reporting obligations. However, the total cost of compliance may be difficult to quantify. In December 2009, the Law Society responded to a call for evidence as part of a Government review of the Money Laundering Regulations 2007. The Law Society conducted a costs survey of its members in 2008 and highlighted the problems inherent in estimating the cost of compliance with the anti-money laundering regime. Their members identified difficulties in quantifying costs in relation to matters such as monitoring clients transactions for warning signs and discussing suspicions and internal reports in deciding whether or not a SAR is required to be made.

1.22 The Law Society reported that on average most firms were spending around four hours each week on discussing suspicions and making disclosures. In terms of time spent by the person responsible for making suspicious activity reports (the "nominated officer"), 50% said it cost them up to £500 a year, the top 25% said it cost them £7,500 or more, with one firm reporting costs of around £164,000. In 2009, a further survey was conducted of some of the top 100 firms. Of the 21 firms that responded, cost estimates for a year ranged from £4,000 to £300,000 in lost fee earner and chargeable time. Total expenditure on quantifiable anti-money laundering compliance costs for each of the firms ranged from £26,800 to £1,035,000 per year. For all 21 firms combined, it was

---

24 "Individual institutions are dedicating very large sums of money to fulfilling their statutory obligations- as much as £36 million a year from one bank." HL Paper 132-1 *Money Laundering and the financing of terrorism – European Union Committee*, Session 2008-2009, vol 1 at para 124.

25 Joint Home Office and HM Treasury *Action Plan for anti-money laundering and counter-terrorist finance* (2016), para 2.1.

26 Corporation of London, *Anti-Money Laundering Requirements: Costs, Benefits and Perceptions* (June 2005), p 9.

27 Corporation of London, *Anti-Money Laundering Requirements: Costs, Benefits and Perceptions* (June 2005), p 4.

almost £6.5 million.[28] These figures exclude the broader costs of anti-money laundering systems development, conducting due diligence, training and staff salaries which may be substantial in larger organisations.

1.23 As we will discuss in Chapter 5, whilst the legal sector does not produce the same volume of SARs as the financial sector, the SARs that are submitted may be more complex in nature. The amount of resources required to conduct due diligence and lodge these disclosures may not be proportionate to the value of the criminal property involved or the seriousness of the crime in every case.

1.24 In addition to the costs to the private sector, it is of fundamental importance that law enforcement agencies' resources are deployed appropriately. The NCA, which has responsibility for overseeing the UKFIU, has confirmed that the volume of SARs is increasing. In its most recent annual report, the NCA highlighted a substantial growth in the total number of SARs and the number of cases where consent had been requested.[29]

1.25 On average, 2000 SARs are received per working day by the UKFIU. Of this figure, on average 100 will be SARs seeking consent to proceed with a financial transaction ((now referred to by the UKFIU as a defence against money laundering or "DAML" SARs and defence against terrorist financing or "DATF" SARs).[30] 25 members of staff are dedicated to processing DAML and DATF SARs at the UKFIU. Increases in the intake of SARs have a consequent impact on processing times. This is a pressing problem where further information is required because the SAR is of poor quality or where a SAR requires input from one of the law enforcement agencies. Based on the current volume of DAML SARs, senior managers spend approximately 20-30% of their time making decisions on consent.[31] All stakeholders we have spoken to felt that the consent process was overburdened and leads to delay.

1.26 Where SARs are unnecessary, of little practical effect, or simply of poor quality, essential resources are diverted from the investigation and prosecution of crime. As this paper will explain, these issues have substantial consequences for both the private sector, law enforcement agencies and the public.

1.27 To remedy some of the most pressing problems, the Law Commission is asking consultees for their views on the suitability of a range of proposed solutions.

---

28 The Law Society, The costs and benefits of anti-money laundering compliance for solicitors: Response by the Law Society of England and Wales to the call for evidence in the Review of the Money Laundering Regulations 2007 (December 2009), pp 25 to 27.

29 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) p 6.

30 These Consent SARs are now referred to as "Defence Against Money Laundering" ("DAML") SARs or "Defence Against Terrorism Financing" ("DATF") SARs.

31 Interviews with UK FIU Staff on 28 March 2018.

THE CONSULTATION PAPER

The purpose of the paper

1.28 The consultation paper has three principal aims: to identify the most pressing problems; consult on reforming the consent regime; and to generate and consider ideas for long-term reform. Our proposals are intended to improve the prevention, detection and prosecution of money laundering and terrorism financing in England and Wales.[32] We will consider whether the current regime is proportionate and efficient.

1.29 After extensive fact-finding meetings with stakeholders, the following issues are noted as causing particular difficulties in practice:

(1) the large volume of disclosures to the UKFIU[33]

(2) the low intelligence value and poor quality of many of the disclosures that are made in accordance with the present legal obligations;

(3) the misunderstanding of the authorised disclosure exemption by some reporters;

(4) abuse of the authorised disclosure exemption by a small number of dishonest businesses and individuals;

(5) defensive reporting of suspicious transactions leading to high volume reporting and poor quality disclosures;

(6) the overall burden of compliance on entities under duties to report suspicious activity; and

(7) the impact of the suspension of transactions on reporting entities and those that are the subject of a SAR.

1.30 In addition, the following legal difficulties have been identified:

(1) the "all-crimes" approach whereby *any* criminal conduct which generates a benefit to the offender will be caught by the regime as "criminal property" and the consequent impact of this on the scope of reporting;

(2) the terminology used in Part 7 of POCA and the meaning of appropriate consent;

(3) the meaning of suspicion and its application by those with obligations to report suspicious activity;

(4) fungibility, criminal property and issues arising from mixing criminal and non-criminal funds;

(5) the extent to which information should be shared between private sector entities;

---

32 Although POCA and Terrorism Act 2000 apply to the UK, this review is limited to England and Wales.

33 634,113 between October 2015 and March 2017, of which 27,471 were DAML SARs. National Crime Agency, Suspicious Activity Reports Annual Report (2017) p 6.

(6) the wide definition of criminal property which applies to the proceeds of any crime and has no minimum threshold value; and

(7) what should constitute a reasonable excuse within Part 7 of POCA.

Scheme of the paper

The current law and its effectiveness

1.31 Chapters 2 and 3 set out the current law surrounding the operation of the suspicious activity reporting regime in relation to money laundering and terrorism financing.

1.32 In Chapter 2, by using the example of a large bank we outline how transactions are monitored by the private sector. We look at required and authorised disclosures, focussing on the obligations on reporters and the process of making disclosures to the UKFIU. We also consider the money laundering offences, including some of the key concepts - such as criminal property, suspicion and criminal conduct - which have generated issues in practice. Further, we consider the available exemptions or defences to those offences. We also outline the tipping off provisions, where an individual risks criminal liability if they inform the subject of a disclosure or investigation that a SAR had been submitted. We examine the issues that arise from these provisions in practice. We summarise the current law on information sharing between the private sector and the NCA. Finally, we look at regulatory requirements on banks and businesses and how their compliance is supervised and monitored.

1.33 In Chapter 3, we consider the objectives of the terrorism financing regime and how they differ from money laundering. We look at the disclosure regime in so far as it differs from our summary in Chapter 2. We examine the terrorist financing offences in the Terrorism Act 2000 and the relevant exemptions or defences. We also look at the tipping off provisions in the context of terrorism financing. We observe that whilst there are similarities across the money laundering and terrorist financing regimes, there are also important differences to consider. In particular, the policy objectives between the two regimes are not necessarily the same; preventing terrorist attacks and disrupting organised criminal activity are separate and distinct aims. The methods used to raise finance for terrorism can also differ from money laundering techniques. For this reason, the types of intelligence that are useful to law enforcement agencies will also be different. Finally, the risk of harm arising from an ineffective counter-terrorism financing regime could be an immediate threat to public safety. We conclude by analysing some of the issues that arise from the current regime and identifying that the principle issue relates to the application of the threshold of suspicion by reporters.

1.34 In Chapter 4, we examine the effectiveness of the current consent regime by analysing the statistics on authorised disclosures[34] and conclude that it is likely that the vast majority of consent SARs do not lead to restraint or seizure of assets.

1.35 We observe that there are two important caveats to this analysis. First, it is difficult to account for disruption of criminal activity. Secondly, there is an absence of data from law enforcement agencies as to when a SAR is integral to an investigation or leads to

[34] Now referred to by the NCA as DAML SARs. This change in terminology will be discussed in Chapters 2 and 12.

a prosecution. We acknowledge that restraint and seizure are not the only measures of effectiveness for SARs. They can assist with an investigation in a number of ways:

(1) by providing intelligence on which to base investigations;

(2) by providing intelligence to assist and develop existing investigations into criminal activity;

(3) by providing intelligence about criminals and their networks which may be of value in the future as part of the general intelligence gathering process; and

(4) by providing reliable information to identify criminals with assets obtained through criminality.

1.36 We observe that the UKFIU receives the highest number of SARs in comparison with other EU States and this trend looks likely to continue. We set out the potential causes for such high reporting volumes. We identify four principal pressures for change: the low threshold for criminality, individual criminal liability, confusion amongst those in the regulated sector as to their reporting obligations and the application of suspicion. We proceed to examine these factors in subsequent chapters.

Pressing problems and possible solutions

1.37 Chapters 5 to 13 identify the most pressing problems with the current law, and identify some provisional solutions to improve the current regime.

Chapter 5

1.38 In Chapter 5, we discuss the "all-crimes" approach to criminal conduct in POCA and the fact that the proceeds of any crime fall within the definition of criminal property. We consider the consequences of this approach and its impact on the volume of reports made. We analyse particular problems faced by the legal sector in identifying what are perceived as "technical" cases of money laundering; where lawyers must comply strictly with their obligations but consider the intelligence value of their disclosure to be low or negligible.

1.39 We examine the alternative "serious crimes" approach and the benefits and disadvantages of moving away from an all-encompassing definition of criminal conduct. We form the provisional view that a change to a serious crimes approach could prove to be problematic and undesirable. However, we invite consultees' comments on the merits of three alternatives to the current "all crimes" approach:

(1) a "serious crimes" approach, based on a list of offences or penalty threshold;

(2) extending the reasonable excuse defence for those who do not make required or authorised disclosures for non-serious crimes (as could be defined in a schedule);

(3) maintaining a formal required disclosure regime for offences on a schedule of serious offences but providing a complementary voluntary scheme for the regulated sector to draw to the attention of the UKFIU any non-serious cases.

Chapter 6

1.40 Chapter 6 considers the key concept of suspicion. We observe that POCA sets the minimum threshold of the mental element for the money laundering offences at suspicion. It is also the minimum threshold for reporting obligations.

1.41 We consider the importance of the concept being understood and applied consistently in the context of reporting volumes and quality of reports. We outline the ordinary meaning of suspicion and its place in the hierarchy of fault in criminal law. We discuss the meaning of suspicion in an investigative context and consider the approaches taken in some other jurisdictions.

Chapter 7

1.42 In Chapter 7, we look at how the concept of suspicion has been applied in the context of money laundering offences. We examine the case law on suspicion and on reasonable grounds to suspect. We also consider industry-led guidance on suspicion and its application.

1.43 We outline the criticisms of the suspicion test in the context of the money laundering offences and the challenges it creates. In particular, we highlight the possibility that suspicion is inconsistently understood and applied by those with reporting obligations. We suggest that this contributes to poor quality disclosures. A poor quality authorised disclosure may still have severe economic consequences for the subject of the disclosure if access to their funds is restricted. We conclude by recognising the need for the system to find a fair balance between the interests of law enforcement agencies, reporters and those who are the subject of a disclosure.

Chapter 8

1.44 Chapter 8 examines the application of the test of suspicion in the context of the disclosure offences. We outline the approach to suspicion in the context of reporting obligations and examine the interpretations of the alternative test of reasonable grounds to suspect. We analyse the two possible interpretations of reasonable grounds to suspect as either a purely objective test, or a mixed test requiring subjective suspicion and objective grounds.

1.45 We consider the approaches of other jurisdictions, focussing on Canada which sets the threshold for reporting at reasonable grounds to suspect and provides guidance on indicators of money laundering. We go on to consider whether the disclosure offences in sections 330 and 331 of POCA set down an objective test, the fairness of such an approach and the likely consequences for reporting volumes. We conclude that it is strongly arguable that "reasonable grounds to suspect" in the context of sections 330 and 331 is a wholly objective test. Finally, we state that there are compelling arguments to suggest that the threshold for liability is too low.

Chapter 9

1.46 In Chapter 9, we bring together all of the analysis in Chapters 6 to 8 and consider the options for reform. We consider whether "suspicion" should be defined in Part 7 of POCA, and identify a number of difficulties with attempting to do that. However, we invite consultees' views on whether and how it might be defined.

1.47 We provisionally propose that the better approach would be for Government to issue formal guidance under a statutory power setting out factors indicative of suspicion. We also provisionally propose that the Secretary of State should introduce a prescribed form pursuant to section 339 of POCA. We invite consultees' views on both of these conclusions.

1.48 Notwithstanding these proposals, we set out the case for amending the reporting threshold and the fault threshold for the disclosure offences to reasonable grounds to suspect in order to make the regime more effective. We outline the benefits of altering the threshold to require a subjective suspicion and objective supporting grounds. We examine whether such a change would comply with the provisions of the 4AMLD and conclude that the position is unclear. At present, we foresee that the UK will continue to comply with its obligations under the 4AMLD subject to the terms of our withdrawal from the EU.

1.49 In relation to the money laundering offences, we come to the view that, in the absence of compelling evidence to the contrary, the fault threshold of suspicion should not be amended. However, we provisionally propose a new defence for the regulated sector. Where an individual in the regulated sector has no reasonable grounds to suspect that property is criminal property within the meaning of section 340, they would not commit an offence. We provisionally conclude that such a change would likely have a positive impact on the overall volume of authorised disclosures (DAML SARs).

1.50 Finally, we form the provisional view that no change should be made to the terrorism financing regime for two reasons. First, the evidence suggests that the main issue in reporting relates to the application of suspicion by reporters, which could be resolved by way of guidance. Those SARs requiring consent (DATF SARs) are submitted in much lower volumes in respect of terrorism financing. Secondly, the objectives of the terrorism financing reporting regime are different to money laundering and may justify a lower threshold. We acknowledge that this creates clearer divide between the two regimes and seek consultees' views on whether this would create problems in practice.

Chapter 10

1.51 Chapter 10 considers the issue of criminal property and identifies problems for the regulated sector arising from the current law where legitimate funds are mixed with criminal funds. In particular, we examine the case law on mixed funds and the problems that arise if adding criminal funds to legitimate funds is considered to taint the whole pot. We highlight the problems faced by banks and the subjects of authorised disclosures when whole accounts are frozen, even where the suspicion relates to only part of the funds in an account.

1.52 We compare approaches to mixed property across POCA and identify a potential way forward. We provisionally propose statutory protection by way of a defence for banks who elect to ringfence the suspected criminal funds whilst they await a decision on consent. We invite consultees to respond to this provisional proposal.

Chapter 11

1.53 In Chapter 11 we consider the scope of reporting on the basis of the current law. On the assumption that an all-crimes approach is retained, we examine ways in which the intelligence value of SARs can be enhanced.

1.54 We identify a list of types of SAR which stakeholders consider to be of little effect or value. We go on to consider the merits of legislative change to account for these types of SARs but provisionally conclude that it would be unworkable. Any legislative amendment defining 'reasonable excuse' in Part 7 of POCA would need to take the form of an exhaustive list. As the list would be liable to change, such an approach risks inhibiting valuable flexibility in the system.

1.55 We provisionally propose that the Government should issue statutory guidance listing matters indicative of the types of things which might be regarded as a 'reasonable excuse' for failing to make a disclosure. We invite consultees' views on whether such guidance would be beneficial in reducing the volume of low-intelligence value SARs.

Chapter 12

1.56 Chapter 12 examines the meaning of 'consent' and problems arising from the interpretation of the term by those with reporting obligations. We outline the problems identified by the NCA which are perceived to arise from the use of the term consent in POCA. We set out the legal consequences of a grant of appropriate consent and consider alternative wording which may better describe the process of obtaining consent. We consider the options for reform. We provisionally propose that there should be a requirement in POCA that Government produces guidance on the term "appropriate consent" under Part 7 of POCA and invite consultees' views on the issue.

Chapter 13

1.57 Chapter 13 examines the current provisions for obtaining and sharing information in relation to money laundering and terrorism financing. We also look at other ways of sharing information such as financial information sharing partnerships. We consider obligations arising under the General Data Protection Regulation and the Data Protection Act 2018.

1.58 We set out stakeholders' views on whether the current provisions are adequate. We analyse the benefits and risks of extending information sharing provisions to allow institutions with reporting obligations to share information with each other even when an unusual transaction does not meet the suspicion threshold. In particular, we look at the risks of debanking and financial disenfranchisement and data protection considerations.

1.59 We conclude that there are strong arguments against allowing private sector institutions to operate at a lower threshold than law enforcement agencies for the obtaining and onward disclosure of information without external scrutiny. We reiterate the arguments presented in Chapters 6 to 9 that suspicion is already a low threshold. We invite consultees' views on whether pre-suspicion information sharing by those in the regulated sector is necessary and/or desirable or inappropriate. If consultees believe it is necessary and/or desirable, we invite thoughts on how such a provision might be formulated in compliance with our obligations under the General Data Protection Regulation. We also invite consultees' views on whether there would be significant benefits to including other entities within the current information sharing partnership (the Joint Money Laundering Intelligence Taskforce or "JMLIT").

Longer term reform

1.60 In Chapter 14, we discuss the significance of our narrow terms of reference and the ideas that we have considered for reforming the current consent regime. Our provisional proposals are based on the current legislative structure, EU obligations and agreed international standards. However, we recognise that alternative models exist. The UK is one of a small number of countries which operates a consent regime and throughout this paper we draw upon the different regimes adopted in a number of other jurisdictions for comparative analysis.

1.61 We confirm that we do not advocate removal of the consent regime. We believe that the adjustments that we have proposed will improve efficiency and provide a better balance between the interests of law enforcement agencies, reporters and those who are the subject of a disclosure. However, we outline what a non-consent model might look like and how it might operate in practice. We examine the benefits and disadvantages of operating without a consent regime.

1.62 We invite consultees' views on the retention of the current regime. In addition, we look at other proposals that may enhance the existing regime. We consider whether the addition of thematic reporting would be beneficial. In doing so, we examine the use of Geographic Targeting Orders in the USA. We invite consultees' views on whether there should be a power to require additional reporting and record keeping requirements targeted at specific transactions.

ACKNOWLEDGMENTS

1.63 In order to ensure we had a thorough grasp on the practical problems inherent in the current regime, we have engaged with a large number of stakeholders in our pre-consultation discussions. We are grateful to them for identifying some of the issues of concern and their ideas on how to improve the current system.

1.64 We are indebted in particular to Rudi Fortson QC (Visiting Professor at Queen Mary, University of London and practising barrister, 25 Bedford Row) who has acted as a consultant on this project.

1.65 This report has been prepared by David Connolly (team manager), Lucy Corrin (team lawyer) and Rebecca Martin (research assistant). Alice Lepeuple (research assistant) undertook invaluable preparatory work during our initial fact-finding stage.

COMMISSION OF INQUIRY
INTO STATE CAPTURE

Chapter 2: Money laundering

2.1 Banks and businesses employ internal monitoring systems to identify unusual or concerning activity. This information is what may generate a suspicion which triggers a reporting obligation. This chapter begins by setting out one type of internal transaction monitoring process. Although the reporting sector extends to professionals and other types of business, we will use the example of a large bank to illustrate the process. We will outline the bank's internal process from the pre-suspicion stage to lodging a Suspicious Activity Report ("SAR"). We will then consider the administrative process of submitting a SAR and what happens at the UK Financial Intelligence Unit ("UKFIU") on receipt of that report. In addition, we will examine:

(1) the types of disclosure that institutions within the private sector make in accordance with their duties under the Proceeds of Crime Act 2002 ("POCA");

(2) the criminal offences for individuals with an obligation to report who may be liable if they fail to disclose when required to do so under the current law;

(3) the money laundering offences and how they can apply to individuals operating businesses in the regulated sector;

(4) the defences or exemptions for money laundering offences available to reporters;

(5) the obligation on reporters not to alert the subject of a SAR that a disclosure has been made to ensure any investigation is not prejudiced ("tipping off");

(6) the ability of reporters to share information between themselves and the UK FIU; and

(7) the additional obligations imposed on individuals with obligations to report under the Money Laundering Regulations 2017 and how they are supervised and regulated.

TRANSACTION MONITORING: THE PRE-SUSPICION STAGE

2.2 In this section, we examine the internal processes that a large reporting bank goes through before submitting a SAR.[1] Most large banks monitor unusual financial activity through a central transaction unit with a nominated officer at the helm. This central unit considers reports which are based on concerns around financial transactions.

2.3 The central transaction unit will receive reports of unusual activity in two formats.

(1) Manual alerts which are internal reports submitted electronically to the transaction unit by any employee of a bank. The employee will have received specific training on identifying unusual activity, what to look for and when to raise

[1] The information in this section of the Paper was obtained during interviews with a large reporting bank based in the UK and is believed to be broadly consistent with the model employed in other banks of the same size.

an internal report. For example, a bank cashier working in a high street branch may be concerned if a customer wants to make a large cash deposit which is out of character with the customer's account activity. They would record their concerns in an internal report and send the report to the central transaction unit to consider.

(2) Automated alerts based on algorithms where the focus is divided into two categories:

(a) Rules which, when applied retrospectively to transactional data, highlight unusual patterns of behaviour based on value, volume and time period. For example, the rules might be set to identify high value transactions over a short period of time.

(b) Rules which look at a customer's activity comparing it to their usual pattern of activity and to their peer group in order to identify anything anomalous or out of character.

2.4 Transactional rules require regular monitoring to ensure that the data produced is informative. They can be affected by general trends and changes in customer behaviour. For example, the introduction of contactless payments required banks to reconsider the normal volume of visa debit transactions as more customers made use of contactless technology to facilitate transactions.

2.5 The vast majority of automated alerts proceed to an investigation, with some immediately discounted if there is a simple explanation, such as a customer enjoying a recent lottery win. All manual alerts are investigated as employees are trained to report only where they have a suspicion. One of the largest reporting banks has a team of 150 investigators who process these alerts. Investigators act as appointed alternates of the nominated officer. One bank confirmed that their investigators underwent six to nine months of training before being in a position to consider and report on transactions.

2.6 At the investigation stage within a bank, financial investigators will pursue a number of different lines of enquiry to establish a) whether the activity is suspicious and requires a report and b) whether consent needs to be sought. Investigators will consider the customer's profile and their transactional associates (i.e who are they paying money to and receiving money from). They will also search for any adverse media articles, for example a news report may confirm that a customer has been convicted of people trafficking which will inform how an investigator views the transactional data. Further enquiries may be made of the customer to see if there is a reasonable explanation. Having consulted multiple sources, the investigator will write a reasoned analysis supported by evidence and make either a required disclosure or an authorised disclosure if appropriate. These decisions are taken under considerable time pressure due to the volume of matters that require investigation. One large bank indicated that their investigators spend 20 minutes on average on each individual case. However, this can be longer if the case is particularly complex.

2.7 Given the scale of transaction monitoring at a large bank, it would be impossible for one nominated officer to oversee every single alert and any subsequent SARs. As we observed in Chapter 1, one large bank estimated the combined monthly total of automated and manual alerts to be in the region of 17,500. The nominated officer relies

on trained and accredited investigators to exercise their judgment. However, nominated officers will be involved in decisions on more complex cases. In smaller scale banks and firms, where the number of reports per annum is much lower, a nominated officer may see every SAR and exercise their own judgment.

2.8 If there is a suspicion of money laundering, the bank will be concerned about funds being dissipated whilst the SAR is being considered. The usual course is to restrict the affected account by placing a block on it. A block is a formal instruction applied to the account which can only be lifted by one of a limited number of officials within the bank. The effect of a block is to stop money going into or out of an account. This means that direct debits, salary payments, income from paid invoices or other funds will not be added or subtracted from the account balance. The customer will not be able to access their funds through an ATM or via online banking. The block acts as an impenetrable wall around the account until it is lifted.

2.9 Once a SAR is lodged, the bank continues to manage the customer and deal with the impact of restricting the customer's account whilst any investigation is ongoing. The customer may be concerned about the impact on their business or being able to make essential payments to meet living expenses. To ensure that they do not "tip off" the customer about their suspicion of criminality and any possible investigation, the bank employ a specific form of words by way of explanation. They are unable to tell the customer the real reason why their account has been restricted. Likewise, they are unable to communicate the reason to branch staff due to the risk of disclosing that an investigation is underway.

THE SUSPICIOUS ACTIVITY REPORTING PROCESS

2.10 At this stage, it is necessary to explain the administrative process once a bank or other reporter submits a SAR to the UKFIU. Before we look at the process, it is important to consider the types of disclosure that the legislation provides for.

Types of disclosure

2.11 The legislation distinguishes between two types of disclosure that are made to the UKFIU (housed within the NCA):

(1) **a required disclosure** provides intelligence to law enforcement agencies. Intelligence disclosures are required where a reporting obligation is triggered under Part 7 despite the reporter not seeking to deal with the criminal property in any way that would offend sections 327 to 329. The failure to lodge a SAR where the conditions for reporting are met is a criminal offence, subject to any statutory exemptions or defences.

(2) **an authorised disclosure** where a person lodges a SAR in which they seek consent to complete a transaction,[2] and benefits from an exemption from the principal money laundering offences if appropriate consent has been given.[3] This means that, were they to be questioned or charged in relation to an offence of money laundering, they could point to their action in lodging a SAR and any grant

[2] Proceeds of Crime Act 2002, s 338.

[3] Proceeds of Crime Act 2002, s 335.

of consent to demonstrate that they had not committed a criminal offence. These SARs are referred to as consent SARs and are now categorised by the UKFIU as either "DAML SARs" (Defence Against Money Laundering) or "DATF" (Defence Against Terrorism Financing) SARs.

2.12 When a SAR is lodged with the UKFIU, it is either sent via the National Crime Agency SAR Online system[4] or bulk data transfer (used by large banks who are submitting a substantial number of reports on a regular basis). A small number of paper reports are submitted each year and whilst they will be accepted, users are encouraged to register and submit their report electronically. POCA also contains a specific provision prohibiting those in the regulated sector from disclosing the fact that they have lodged a SAR where such disclosure is likely to prejudice any investigation triggered by this intelligence. This prohibition, known as "tipping off", will be considered in more detail later in this Chapter.

2.13 There is one SAR form to be submitted regardless of whether a reporter is making a required or an authorised disclosure. The format of the report is not prescribed by law[5] but has developed through practice. The reporter indicates, by ticking a box, whether they are making an authorised disclosure and seeking consent to act.

2.14 All reports are uploaded to the UKFIU's ELMER database. On average, the UKFIU receives 2,000 suspicious activity reports per day, of which approximately 100 will include requests for consent.

The seven-day notice period

2.15 When a SAR is used to make an authorised disclosure, this triggers a statutory seven-working-day notice period during which the UKFIU processes the report and decides whether to grant or refuse consent. This, in effect, pauses any financial transaction and prevents the dissipation of funds. If a reporter were to complete the transaction during this period, they would risk prosecution for one of the principal money laundering offences.

2.16 DAML or DATF SARs in which the reporter ticks the box seeking consent are automatically uploaded onto the "Clear Framework" database in date order of receipt. A specialist team of case officers at the FIU work on consent SARs. Further checks are performed to identify any reports where consent is sought but the box has not been ticked. These result from reporters using incompatible systems or human error. Keyword searches are used to identify these reports and they are manually uploaded onto the Clear Framework database.

2.17 All SARs are submitted in confidence by reporters. They are treated as sensitive and are only accessible by officers working within the Financial Intelligence Unit.[6] As the content of a SAR may only be known to an individual or a small circle of people,

---

4 The NCA SAR online system can be accessed here: https://www.ukciu.gov.uk/(g2rhed55yxdkob2j45qmrne1)/saronline.aspx (last visited 9 April 2018).

5 The power to prescribe the form of disclosures exists in Proceeds of Crime Act 2002, s 339.

6 National Crime Agency, *Operating Procedure: Recording SARs on NCA Core Systems* (Version 2 January 2018) p 1.

dissemination is restricted.[7] They are made available to law enforcement officers who have been trained in handling sensitive data and the consequent need to protect the original source of the information. SARs are stored on the ELMER database for 6 years and may be accessed by law enforcement agencies during that time. The exception to this rule is where a SAR forms part of a criminal justice case in which case its retention is managed with the rest of the case material. In December 2011, all SARs more than six years old were deleted and this deletion process is ongoing. Where a SAR is lodged, but feedback indicates that the suspicious activity (that is subject of the report) is not related to criminality, the UKFIU will delete it.[8] Where there is no indication within the body of the SAR that there is knowledge or suspicion of money laundering or criminal property, the SAR can also be deleted. ELMER currently holds 2.25 million suspicious activity reports.[9]

2.18 All SARs in which the reporter seeks consent are analysed by an officer in the Financial Intelligence Unit. SARs have a large free-text box where the reporter is required to outline the reasons for their suspicion. A set of standard codes, created by the UKFIU, can be used by reporters when submitting a SAR to highlight the reason why they suspect money laundering, although this is voluntary.[10] The officers triage the reports and flag the report with a designation of red, amber or green; the flags indicate the value involved, the level of complexity and risk.[11] Red represents either the highest value, the greatest level of interest by law enforcement agencies or the largest risk; amber is used to designate complexity and green refers to the lowest value and lowest risk cases. Reports seeking consent are allocated to a case officer who analyses the information to check for completeness and creates a case record for the suspicious activity report. Nearly 30% of consent SARs are assessed as green (low value transactions, property transactions or internal transfers between ledgers with no known interest from law enforcement agencies or likely terrorist financing link).

2.19 Following initial analysis, reports which are missing two or more pieces of key information are closed immediately. The reporter is notified that the requirements have not been met. For example, a reporter may omit the nature of their suspicion or fail to identify the suspected criminal property. Reporters are invited to remedy the defects and re-submit if appropriate. The total number of cases which were closed because they did not fulfil the requirements or there had been a misunderstanding of consent was 3,326 between October 2015 and March 2017. This amounts to approximately 12% of the overall number of SARs seeking consent to proceed.

2.20 In some instances, further information is required in relation to a suspicious activity report before it can be processed by a case officer as a SAR where consent is sought. In such circumstances the reporter is contacted by email and asked to respond by a

---

7 Home Office Circular 22/2015 "*Money Laundering: The confidentiality and sensitivity of Suspicious Activity Reports [SARs] and the identity of those who make them*".

8 http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/the-sars-regime (last accessed 22 June 2018).

9 Interview with UKFIU staff.

10 National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2017*, p11.

11 Interview with UKFIU staff.

deadline. UKFIU data shows that further information is required in around10% of SARs.[12] Where further information has to be requested, case officers must still operate within the statutory time limit.

2.21 Once the information is complete, the SAR may be allocated to the appropriate law enforcement agency. Under 40% of consent SARs are referred to a law enforcement agency and are allocated according to the postcode of the SAR. For example, those cases which are triaged and assessed to be 'green' cases will very rarely be sent to law enforcement agencies to consider. Where cases are referred, they will typically be shared with the regional police force for the relevant area where the suspicious activity was reported. That law enforcement agency decides what, if any action, it proposes to take. Any recommendation from the law enforcement agency is taken into account by the UK Financial Intelligence Officer who makes the final decision on granting or refusing consent.[13]

2.22 Of the 27,471 SARs where consent was sought between October 2015 and March 2017, 74% were granted, 6% were refused and 12% resulted in deemed consent (the circumstances in which deemed consent will apply will be considered later in this Chapter). 8% were identified as wrongly seeking consent (approximately 2197 SARs).[14] During this time period, the average turnaround time for responses to reporters for all requests was between 5.8 and 6.2 days.[15] If consent is refused, a moratorium period of 31 days begins, allowing law enforcement agencies additional time to investigate and consider any further action. For example, the police might make an application to restrain criminal funds or an application to monitor a bank account as a result of the intelligence provided.[16]

The moratorium period

2.23 As noted above, if a request for consent is refused during the seven-day notice period, a statutory moratorium period of 31 calendar days begins. The reporter is prohibited from taking further action whilst the investigation continues, or does so without the protection afforded by a grant of consent.

2.24 If no response is received by the expiry of the moratorium period, the reporter is treated as if they had been given appropriate consent. This means that they can act in a way (towards the property about which they were suspicious) that would ordinarily be an offence under section 327, 328 or 329 of POCA. In the ordinary course of events they will commit no offence by doing so. However, it is unclear whether the lodging of a deliberately defective SAR would provide a defence.

2.25 Under the original provisions of POCA, the UKFIU had a statutory maximum of 38 days to respond to an authorised disclosure. This period was made up of the initial seven-

---

12 Interview with UKFIU staff.

13 Interview with UKFIU staff.

14 Interview with UKFIU staff.

15 National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2017*, p 19.

16 This is subject to the new power in the Criminal Finances Act 2017 for a Crown Court judge to extend the moratorium period. See Proceeds of Crime Act 2002, s 335(6) considered below.

day notice period and a further 31-day moratorium period.[17] However, there were growing concerns that this was too short. The moratorium period could expire allowing funds to be dissipated before an investigation had progressed sufficiently to determine whether proceedings should be undertaken.

2.26 The Criminal Finances Act 2017 introduced new powers to extend the moratorium period beyond the initial 31 days provided for in the Proceeds of Crime Act 2002.[18] The aim was to provide law enforcement agencies with an appropriate amount of time to undertake investigations without funds being dissipated particularly in complex transactions, such as overseas investigations. The amendments provide a judge sitting in the Crown Court with a power to authorise the extension of the moratorium period for periods of up to 31 days. This process can be repeated up to a total of 186 calendar days from the end of the initial 31-day moratorium period.[19]

2.27 The test to be applied by the judge in exercising that discretion is whether the investigation is being carried out diligently and expeditiously, *but despite that expedition* further time is needed for conducting the investigation, *and* it is reasonable in all the circumstances for the moratorium period to be extended.[20]

2.28 Rule 47.64 of the Criminal Procedure Rules requires notice to be served on the 'respondent'. Whilst the respondent would usually be the person who made the disclosure, the definition of respondent includes any other person who appears to the applicant to have an interest in the property that is the subject of the disclosure.[21] This may include the owner of the property or a third party such as an intended recipient of funds.

2.29 The court may require the applicant to serve a copy of the application on the respondent. Equally a judge may, in the exercise of their discretion, determine that information should be withheld from a respondent,[22] dispense with any requirement for service[23] or exclude them or their legal representative from the hearing.[24]

2.30 Section 333D(1)(aa)[25] provides that tipping off is permitted for the purposes of proceedings to extend the moratorium period.[26] This takes into account the provision

---

17 It is important to note that the actual period will be longer given the combination of "working days" (notice period) and calendar days (moratorium period).

18 Proceeds of Crime Act 2002, s 335(6).

19 By the Criminal Finances Act 2017, Part 1, s 10(2) (s 335(6A) in force, October 31, 2017, subject to transitional provisions specified in SI 2017 No.991 reg 3(1)). See Proceeds of Crime Act 2002, ss 335(6A), 336A, B, C, and D. See Home Office Circular 008/2018 [*Criminal Finances Act: extending the moratorium period for suspicious activity reports].*

20 Proceeds of Crime Act, s 336A.

21 Proceeds of Crime Act, s 336D.

22 Criminal Procedure Rules, r 47.65(3)(a).

23 Criminal Procedure Rules, r 47.63(8)(b).

24 Proceeds of Crime Act 2002, ss 336B(3)(a) and 336D(3)(a).

25 Proceeds of Crime Act 2002. This section provides for "other permitted disclosures".

26 Proceeds of Crime Act 2002, s 336A.

for notice to be given to the subject of a disclosure outlined above. During this period the tipping off offence under section 333A of the Proceeds of Crime Act 2002 is disapplied.[27] Home Office Circular 008/2018 states that where an application to extend is made, a person does not commit a "tipping off" offence[28] if:

(1) the disclosure is made to a customer or client of the person;

(2) the customer or client appears to the person making the disclosure to have an interest in the relevant property; and

(3) the disclosure contains only such information as is necessary for the purposes of notifying the customer or client that the application to extend has been made.

2.31 While the court can extend the period of the moratorium, decisions on whether to grant or refuse consent rest with the UKFIU, on recommendation from the relevant law enforcement agency.[29]

THE FAILURE TO DISCLOSE OFFENCES

2.32 If a reporter fails to lodge a SAR in accordance with their obligations under Part 7 of the Proceeds of Crime Act 2002, they may be liable for prosecution for one of three disclosure offences, depending on their status and whether they were acting within or outside the regulated sector.[30]

2.33 The regulated sector is defined in Schedule 9 of the Proceeds of Crime Act 2002 and the original definition has been amended by various legislative provisions and EU law. Broadly, the regulated sector encompasses businesses where their activity presents a high risk of money laundering or terrorism financing. Businesses may be included within the definition by virtue of the type of activity they undertake. For example, the acceptance by a credit institution of deposits or other repayable funds from the public, or the granting by a credit institution of credits for its own account brings banks into the regulated sector. A firm of solicitors who undertake conveyancing work would be included as they are "participating in the buying or selling of real property" and would fall within the definition in Schedule 9. In addition, those who trade in goods are brought within the regulated sector whenever a transaction involves the making or receipt of a payment or payments in cash of at least 10,000 euros in total. This threshold applies whether the transaction is executed in a single operation or in several operations which appear to be linked, by a firm or sole trader who by way of business trades in goods. However, as the nature of the activity is relevant, it is possible a business may

---

27 Proceeds of Crime Act 2002, ss 333A and 333D.

28 Home Office Circular 008/2018, *Criminal Finances Act: extending the moratorium period for suspicious activity reports*, para 18. It is of note that the paragraph refers to a person not committing an offence under 336D; it is assumed that this is an error as the tipping off offence is in section 333A as the preceding sentence in the paragraph confirms.

29 Home Office Circular 0124/2018, *Criminal Finances Act 2017 - Power to extend moratorium period sections 336A-336C,* para 26.

30 Proceeds of Crime Act 2002, ss 330 to 332.

undertake some work which falls within the definition of the regulated sector and other work which does not.[31]

Failure to disclose by those working within the regulated sector

2.34 Section 330 applies to a person acting in the "course of a business in the regulated sector" who fails to make a "required disclosure". Disclosure is required where four conditions are met:

(1) he or she "knows or suspects" or has "reasonable grounds for knowing or suspecting") that another person is engaged in "money laundering";

(2) the information or other matter on which his or her knowledge or suspicion is based or provides reasonable grounds for suspicion must have come to him or her in the course of business in the regulated sector;

(3) he or she can identify the person engaged in money laundering or the whereabouts of any of the laundered property; or

(4) he or she believes, or it is reasonable to expect him or her to believe, that the information or other matter will or may assist in identifying the person or the whereabouts of any of the laundered property.

2.35 The information which the reporter is required to disclose is:

(1) the identity of the person, if he or she knows it;

(2) the whereabouts of the laundered property, so far as he or she knows it;

(3) information that will or may assist in identifying the other person or the whereabouts of any of the laundered property.

2.36 An offence is committed when a person does not make the required disclosure to either the nominated officer or the UK Financial Intelligence Unit as soon as is practicable after the information comes to him or her.[32]

Failure to disclose by nominated officers working in the regulated sector

2.37 Section 331 applies to "nominated officers" who operate in the "regulated sector". A nominated officer is a person who is nominated within a firm, company or other organisation to submit SARs on their behalf to the UKFIU. If an employee has a suspicion, the nominated officer must evaluate the information reported and decide whether, independently, they have knowledge, or a suspicion or should have reasonable grounds to suspect money laundering based on what they have been told.

2.38 The nominated officer's obligation to disclose only arises where they receive a required disclosure from another person (pursuant to section 330 of the Proceeds of Crime Act 2002) informing them of a knowledge or suspicion of money laundering. For example, a solicitor in a law firm may disclose their suspicion that a client is engaged in money

---

31 Proceeds of Crime Act 2002, Schedule 9.

32 Proceeds of Crime Act 2002, s 330.

laundering to the firm's money laundering reporting officer (the "nominated officer"). In practice, the nominated officer acts as a filter before a suspicious activity report is submitted. It will be the responsibility of the money laundering reporting officer to decide if they are obliged to lodge a SAR by considering whether the following three conditions apply:

(1) they know or suspect or have reasonable grounds to know or suspect, that another person is engaged in "money laundering";

(2) the information or other matter on which their knowledge or suspicion is based, or which gives them reasonable grounds for suspicion, came to them in consequence of a disclosure made under section 330; and

(3) he or she:

(a) knows the identity of the person engaged in money laundering or the whereabouts of any of the laundered property, in consequence of a disclosure made under section 330; or

(b) the person or whereabouts of the laundered property can be identified from the information of other matter; or

(c) they believe, or it is reasonable to expect them to believe, that the information or other matter will or may assist in identifying the person or the whereabouts of any of the laundered property.

2.39 The information which the reporter is required to disclose is:

(1) the identity of the person, if disclosed in the section 330 report;

(2) the whereabouts of the laundered property, so far as disclosed in the section 330 report; and

(3) information that will or may assist in identifying the other person or the whereabouts of any of the laundered property.

2.40 An offence is committed when a person does not make the required disclosure to either the nominated officer or the UKFIU as soon as is practicable after the information comes to him or her.[33]

Failure to disclose by other nominated officers

2.41 Section 332 applies to nominated officers other than those acting within the regulated sector. For example, a high street chain of jewellery shops may typically conduct transactions which fall below the transaction threshold of 10,000 Euros necessary to bring them within the regulated sector. If the nominated officer of this high street chain fails to make a required disclosure in accordance with section 332, they are at risk of criminal liability under that section.

[33] Proceeds of Crime Act 2002, s 331.

2.42 Disclosure is required where the following three conditions are made out:

(1) he or she knows or suspects that another person is engaged in money laundering;

(2) the information or other matter on which his or her knowledge or suspicion is based came to him or her in consequence of a disclosure either under section 337 (a protected disclosure) or 338 (an authorised disclosure); and

(3) he or she:

(a) knows the identity of the person, or the whereabouts of any laundered property in consequence of the disclosure they received; or

(b) the person, or the whereabouts of any of the laundered property, can be identified from the information or other matter received; or

(c) he or she believes, or it is reasonable to expect him or her to believe, that the information or other matter will or may assist in identifying the person or the whereabouts of any of the laundered property.

2.43 The information which the reporter is required to disclose is:

(1) the identity of the person, if disclosed to him or her;

(2) the whereabouts of the laundered property, so far as disclosed to him or her;

(3) any information or matter disclosed to him or her that will or may assist in identifying the other person or the whereabouts of any of the laundered property.

2.44 An offence is committed when a person does not make the required disclosure to either the nominated officer or the UKFIU as soon as is practicable after the information comes to him or her.[34]

Penalty

2.45 The maximum penalty is, on summary conviction, imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or both. On indictment, the maximum penalty on conviction is imprisonment for a term not exceeding five years, or a fine or both.[35]

Exemptions from the failure to disclose offences

2.46 A person does not commit an offence if one of the following exemptions applies:

[34] Proceeds of Crime Act 2002, s 332.

[35] Proceeds of Crime Act 2002, s 334.

(1) **Reasonable excuse**: In respect of sections 330, 331 and 332, he or she has a reasonable excuse for not making the required disclosure;[36]

(2) **Statutory legal privilege:** In relation to section 330, no offence is committed where he or she is a professional legal adviser and the information came to him or her in privileged circumstances (statutory legal privilege) where there was no intention to further a criminal purpose.[37] Privileged circumstances will arise where the information is communicated or given to a professional adviser by a client (or a representative of a client) in connection with the giving of legal advice to the client, or by a person seeking legal advice from the advisor or by a person in connection with legal proceedings or contemplated legal proceedings.[38] There is an additional exemption for those who provide assistance or support to a professional advisor who will also be protected from liability where the information is covered by privilege. However, gaining the benefit of this exemption is dependent upon the information in fact being legally privileged, something that the person will not necessarily be in a position to ascertain readily.[39]

(3) **Inadequate training by employer**: In respect of section 330, he or she does not know or suspect that another person is engaged in money laundering and they had not been provided with appropriate training by their employer.

(4) **Money laundering outside the UK**: In respect of sections 330, 331 and 332, he or she knows or believes on reasonable grounds that the money laundering is occurring in a particular country or territory outside the UK and it is not unlawful there (or of a description prescribed in an order made by the Secretary of State).

2.47 In deciding whether an offence has been committed under section 330 or 331 by a person working in the regulated sector, a court must consider whether he or she had followed any guidance issued by a supervisory authority, or other appropriate body which has been approved by HM Treasury.[40]

2.48 There are multiple sector-specific guides to the law in this area. For example, HM Treasury has approved guidance issued by the Joint Money Laundering Steering Group ("JMLSG") for financial institutions, the Consultative Committee of Accountancy Bodies ("CCAB") for auditors, insolvency practitioners, external accountants and tax advisers and the Legal Sector Affinity Group ("LSAG") for independent legal professionals and staff who work in a law practice. Each is intended to be tailored to the sector it represents and provide employees and professionals with guidance on how to comply with the law.

---

36 Proceeds of Crime Act 2002, ss 330(6)(a), 331(6) and 332(6).

37 Proceeds of Crime Act 2002, ss 330(6)(b), 330(10) and 330(11).

38 Proceeds of Crime Act 2002, s 330(10).

39 Proceeds of Crime Act 2002, s 330(7B).

40 HM Treasury, *Approved Guidance on Money Laundering Controls and Terrorist Financing* available at https://www.gov.uk/government/publications/approved-guidance-on-money-laundering-controls-and-terrorist-financing (last accessed on 16 April 2018).

Issues arising from the failure to disclose offences

2.49 Five important issues arise from an examination of the disclosure offences:

(1) Whilst "nominated officers" are those employed on behalf of a company or firm to consider unusual or suspicious activity and make reports to the UK Financial Intelligence Unit, section 330 also places a reporting obligation on all employees in the regulated sector. The breadth of this provision would include, for example, an employee of a bank processing cash deposits for a customer at a high street branch.

(2) The Act potentially imposes a greater burden on those operating within the regulated sector in sections 330 and 331 with the addition of 'reasonable grounds to suspect'. In addition to triggering a reporting obligation where there is knowledge or suspicion, there is an issue around the meaning of "reasonable grounds to suspect" and whether it may imposes liability for negligence. This will be considered later in this Paper. Furthermore, ordinary employees as well as nominated officers are at risk of prosecution.

(3) Sections 330 and 331 are offences which seek to encapsulate the same conduct performed with one of several states of mind of very different levels of culpability, but which impose the same maximum penalty imprisonment. There remains an issue as to what behaviour these offences may criminalise.

(4) No statutory guidance has been given as to what constitutes a reasonable excuse. The "reasonable excuse" defence has not been tested by the courts. This creates a vacuum that sector specific guidance has attempted to fill. However, approaches to what may constitute a reasonable excuse are not consistent across sector guidance. For example, guidance given to accountants confines a reasonable excuse for failing to disclose narrowly in terms of threats to personal safety or duress.[41] Guidance to the legal sector gives the following examples of what may constitute a reasonable excuse for failure to disclose:[42]

(a) you are prevented from disclosing if your knowledge or suspicion is based on privileged information and legal professional privilege is not excluded by the crime/fraud exception; or

(b) if it is clear that a regulator or enforcement authority (in the UK or elsewhere) is already aware of the suspected criminal conduct or money laundering and the reporter does not have any additional information which might assist the regulator or enforcement authority, or

---

41 CCAB [*Anti-money laundering guidance for the accountancy sector*] (2018), para 2.2.2, "this is likely to be defined narrowly, in terms of personal safety or security, and so very rare." Para 2.2.3, simply states that there is "no de minimis" value for reporting. Para 3.5.14, a lack of relevant training for an employee and para 6.1.19, "…it is anticipated that only relatively extreme circumstances – such as duress or threats to safety – would be accepted."

42 Legal Sector Affinity Group, *Anti-Money Laundering Guidance for the Legal Sector* (2018), pp 91 to 92.

(c) if the only information that a reporter would be providing for the purposes of an authorised disclosure or a report under section 330 is information entirely within the public domain, or

(d) if all the suspected predicate offending occurs outside the UK and all the suspected money laundering occurs outside the UK and there is otherwise no UK nexus to the suspected criminality.

(5) The existence of multiple sector-specific guides drafted by various supervisory authorities in this area may make it difficult for reporters to understand their obligations. It also creates inconsistency in approach across different sectors. This may offer less comfort and protection to those making decisions on reporting who are at risk of prosecution.[43]

THE MONEY LAUNDERING OFFENCES

2.50 Part 7 of POCA creates three principal money laundering offences.[44]

2.51 The offences in sections 327, 328 and 329 of POCA are intended to criminalise specific acts of money laundering. A person commits an offence of money laundering if he or she:

(1) conceals; disguises; converts; transfers; or removes criminal property from England and Wales, Scotland or Northern Ireland; or[45]

(2) enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person;[46] or

(3) acquires criminal property; uses criminal property; or has possession of criminal property.[47]

2.52 A criminal may seek to launder the proceeds of his own criminal activity, for example an offender may steal a car and lend it to a friend who, with the requisite knowledge or suspicion of its origins, makes use of the vehicle. This could amount to using criminal property under section 329 of the Proceeds of Crime Act 2002.

2.53 However, the offences are not restricted in their application to the original offender. A family member of the drug dealer may accept cash from the offender and place it into their own bank account to disguise the source of the money. This would amount to an offence under section 327. Alternatively, if they accepted a cash gift and spent the

---

43 Proceeds of Crime Act 2002, ss 330(6)(a), 331(6), and 332(6). For example, see JMLSG Board Approved Final Guidance Part 1 December 2017 at paras 6.47 and 6.52.

44 Proceeds of Crime Act 2002, s 340(11) and ss 327 to 329.

45 Proceeds of Crime Act 2002, s 327.

46 Proceeds of Crime Act 2002, s 328.

47 Proceeds of Crime Act 2002, s 329.

money on an expensive watch, an offence under section 327 or 329 may have been committed.

2.54 Professionals can also be involved in laundering the proceeds of crime. A conveyancing solicitor who (with the requisite mens rea) facilitates a property purchase by the drug dealer using their criminal funds as a deposit may commit an offence under section 328.

2.55 It is immaterial who carried out the original crime which generated the illicit funds (known as the "predicate offence"), or who benefited from it (whether it was one person or many more).[48]

Penalty

2.56 The maximum penalty for each of the principal money laundering offences is substantial. A person guilty of an offence under either section 327, 328 and 329 is liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or both. On indictment, the maximum penalty is imprisonment for a term not exceeding 14 years, or a fine, or both. In the event of conviction, a court may proceed to consider confiscation of the offender's benefit from criminal conduct.[49]

Key concepts

2.57 There are three important concepts common to the money laundering offences which are examined in detail below: "criminal property", "suspicion" and "criminal conduct".

Criminal property

2.58 Each of the principal money laundering offences is conditional upon the action in question (e g transferring, or using) being done in relation to "criminal property"'. If the property is not criminal in nature, the principal offences in sections 327 to 329 of the Proceeds of Crime Act 2002 are not committed.

2.59 For property to be "criminal", it must satisfy two conditions:

(1) it must constitute a person's benefit from criminal conduct or represent such a benefit (in whole or in part and whether directly or indirectly); and

(2) the alleged offender must know or suspect that it constitutes or represents such a benefit.[50]

2.60 A person will be considered to have benefitted from criminal conduct if he obtains some property (or other financial advantage) as a result of or in connection with the conduct.[51]

---

48 Proceeds of Crime Act 2002, s 340(4).

49 Subject to the conditions in Proceeds of Crime Act 2002, s 6(1). Sections 327 and 328 (but not 329) are criminal lifestyle offences in accordance with Proceeds of Crime Act 2002, s 75 and Schedule 2.

50 Proceeds of Crime Act 2002, s 340(3), (4).

51 Proceeds of Crime Act 2002, s 340(5) to (7).

2.61 Criminal property has been broadly defined by the legislation. Whilst criminal proceeds may take the form of cash, more sophisticated levels of laundering are accounted for. The definition would include a house or a car purchased with the proceeds of criminal activity. Criminal property is not restricted to physical money in the form of notes and coins. A credit balance on a bank account or equity shares in a company would fall within this wide definition.[52]

Suspicion

2.62 Suspicion is a key component of the money laundering offences. It is the minimum mental state required for the commission of an offence under sections 327, 328 and 329: a person must suspect that the property in question is criminal property.[53] The fact that a person suspects that property is criminal may, depending on the circumstances, also trigger a reporting obligation under sections 330, 331 and 332 which will be considered below. In the absence of a statutory definition or guidance, it has been left to the courts to determine what "suspicion" means.

2.63 In the context of money laundering, the leading authority on the meaning of suspicion is *R v Da Silva.*[54] In this case, the Court of Appeal considered the correct interpretation of suspicion within the meaning of section 93A(1)(a) of the Criminal Justice Act 1988 (the predecessor to the Proceeds of Crime Act 2002):

> What then does the word "suspecting" mean in its particular context in the 1988 Act? It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be "clear" or "firmly grounded and targeted on specific facts", or based upon "reasonable grounds".[55]

2.64 In *Da Silva*, the Court considered whether the statute required reasonable grounds for a suspicion, but rejected that interpretation. Without a statutory definition or guidance as to the meaning of suspicion, we make two important observations at this point which will be discussed further below:

(1) Suspicion is a low threshold if it requires only a possibility which is more than fanciful. Whilst this provides simplicity, it may inadvertently catch those whose activity is simply unusual or not commonplace. This will affect the quality of reports submitted.

(2) Without a clear definition, guidance or a requirement for reasonable grounds, suspicion can be inconsistently applied by those who have to decide whether or not to report their concerns.

---

52 Proceeds of Crime Act 2002, s 340(9).

53 Proceeds of Crime Act, s 340(3)(b).

54 [2006] EWCA Crim 1654, [2006] 2 Cr App R 35.

55 [2006] EWCA Crim 1654, [2006] 2 Cr App R 35.

Criminal conduct

2.65 Criminal conduct is defined broadly as conduct which "constitutes an offence in any part of the United Kingdom".[56] The UK's approach to money laundering is described as an 'all-crimes' approach. That means simply that laundering the proceeds of *any crime* of *any value* whatsoever will amount to the offence: from a multi-million pound fraud to the simple act of taking a bicycle without the permission of the owner.[57] It is not limited to serious crimes, certain types of offending, or those punishable with imprisonment.

2.66 Criminal conduct is conduct which:

(a) constitutes an offence in any part of the United Kingdom; or

(b) would constitute an offence in any part of the United Kingdom if it occurred there."[58]

2.67 Conduct abroad which would be legal in that country but unlawful somewhere in the United Kingdom is sufficient. For example, conduct that took place in Egypt might amount to fraud in the UK and would therefore be criminal conduct for the purposes of section 340 of POCA. However, the limited exceptions to this will be discussed further at 2.73 below.[59]

2.68 There is no temporal limit to criminal property; it does not matter whether the criminal conduct occurred before or after the passing of POCA. If the property is generated by criminal activity at any stage, its use in any of the ways described in sections 327 to 329 is proscribed. For example, if an offender stole a painting and kept it for decades, it would remain criminal property regardless of the passage of time. It is an all crimes "for all time" approach.

EXEMPTIONS OR DEFENCES TO THE PRINCIPAL MONEY LAUNDERING OFFENCES

2.69 The legislation identifies a number of circumstances where an offence will not be committed and for this reason, they are referred to in this paper as "exemptions", although the term "defences" has also been applied in the literature on this topic.[60] Five exemptions apply to all three of the principal money laundering offences,[61] and one further exemption applies in respect of section 329 only.

---

56 Proceeds of Crime Act 2002, s 340.

57 Theft Act 1968, s 12(5) and (6). Punishable on summary conviction with a fine not exceeding level 3 on the standard scale.

58 Proceeds of Crime Act 2002, s 340.

59 See Serious Organised Crime and Policing Act 2005, s 102 and the Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006, SI 2006 No 1070.

60 We are using these terms to mean simply that where a "defence" applies, this means that an individual has committed all of the elements of the offence, but if certain factors are present, they may be absolved of criminal liability. An exemption is different as it means that an individual commits no offence if their conduct falls within a specified category.

61 There may be some difference in statutory language depending on whether the exemption applies to section 327, 328 or 329.

The five common exemptions

2.70 Five exemptions apply to all of the money laundering offences. The principal focus of this paper is on the authorised disclosure exemption which will be considered in detail below. In summary, an offence is not committed under sections 327, 328 and 329 if one of the following exemptions applies.

(1) **Authorised disclosure:** [62] A money laundering offence is not committed under sections 327 to 329 of the Proceeds of Crime Act 2002 where a person makes an "authorised disclosure" to the authorities and acts with "appropriate consent". This exemption would apply where, for example, a bank official suspects criminal property is in an account. That fact can be disclosed to the authorities and consent obtained to continue to process relevant transactions.

(2) **Reasonable excuse:** [63] This exemption applies where a bank or business suspected it was dealing with criminal property, intended to disclose that fact to the authorities but failed to do so. If there was a reasonable excuse for their failure to disclose they will still benefit from the exemption. We will examine the reasonable excuse exemption in more detail below.

(3) **Carrying out a law enforcement function:** [64] This exemption applies to police officers and financial investigators who are dealing with criminal property in the course of their work. For example, where a law enforcement agency has to deal with criminal property, they are protected because they are carrying out a function relating to the enforcement of the Proceeds of Crime Act 2002.

(4) **Overseas conduct which is lawful there:** [65] Professionals may identify evidence suggesting that a criminal offence was committed outside the UK. For example, where an accountant knows, or believes on reasonable grounds, that criminal conduct occurred in a particular country or territory outside the United Kingdom, and the relevant criminal conduct was not at the time it occurred, unlawful under the criminal law applied in that country or territory. The scope of the defence is limited to cases where the predicate conduct in question constitutes an offence punishable by imprisonment for a maximum term not exceeding 12 months in any part of the United Kingdom, if it occurred there, with some specific exclusions.[66]

(5) **Exemption for banks and other deposit-taking bodies:** The legislation allows a bank official who suspects criminal property is represented in an account to continue to perform transactions as long as they are under the threshold amount

---

62 Proceeds of Crime Act 2002, ss 327(2)(a), 328(2)(a), 329(2)(a) and 338.

63 Proceeds of Crime Act 2002, ss 327(2)(b), 328(2)(b) and 329(2)(b).

64 Proceeds of Crime Act 2002, ss 327(2)(c), 328(2)(c) and 329(2)(d).

65 Proceeds of Crime Act 2002, ss 327(2A)(b)(ii), 328(3)(b)(ii) and 329(2A)(b)(ii).

66 See Serious Organised Crime and Policing Act 2005, s 102 and the Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006, SI 2006/1070. The exclusions are an offence under the Lotteries and Amusements Act 1976, or an offence under section 23 or 25 of the Financial Services and Markets Act 2000.

which is currently set at £250. This permits small payments to meet living expenses or cash withdrawals to be made and has two benefits. First, it means no offence is committed where the value is below the threshold. Secondly, it avoids the administrative burden of seeking consent in each case. A higher threshold can be requested and authorised.[67]

During our pre-consultation discussions, it has been suggested that given the likely average payments necessary to meet living expenses such as mortgage or bill payments, particularly in London, the threshold amount appears low. At its current level it seems unlikely to reflect realistic financial commitments. In the case of mortgage payments where the money is being applied to real (immoveable) property, the justification for such a low threshold is questionable.

The adequate consideration exemption

2.71 A further exemption applies in respect of section 329 only (acquiring, using or having possession of criminal property), where an individual acquires, uses or has possession of the property for adequate consideration. This exemption is intended to cover tradespeople who are paid for goods and services. It does not apply where an individual provides goods and services which they know or suspect may help another to carry out criminal conduct.[68] In these circumstances, an offence is not committed by a tradesperson.. CPS guidance states that this exemption also applies to professional advisors who receive money for or on account of costs from a client or third party on the client's behalf.[69]

The authorised disclosure exemption

2.72 The authorised disclosure exemption[70] is at the heart of the consent regime. It is intended to protect those who will inevitably encounter suspected criminal property in the course of business or in a professional capacity. No criminal offence is committed where an authorised disclosure is made and appropriate consent to proceed with an act otherwise proscribed by sections 327 to 329 of the Proceeds of Crime Act 2002 is given.

2.73 For a disclosure to be authorised, it must be made to either a nominated officer (a person nominated within a company, firm or other organisation to receive reports of suspicious activity), a constable, or a customs officer. The matter disclosed is that the property is known or suspected to be criminal property.

2.74 The timing of the disclosure is important. To benefit from the exemption, the disclosure must be made either:

---

67 Proceeds of Crime Act 2002, s 339A.

68 Proceeds of Crime Act 2002, ss 329(2)(c) and 329(3)(c).

69 See also *R v Afolabi* [2009] EWCA Crim 2879. Legal Affinity Group Guidance on anti-money laundering (2018), para 6.5.2. CPS Guidance to Prosecutors, *Proceeds of crime Act 2002 Part 7 – Money Laundering* https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences (last accessed 4 June 2018).

70 Proceeds of Crime Act 2002, ss 327(2)(a), 328(2)(a) and 329(2)(a).

(1) in advance of a transaction; or

(2) during a transaction if the reporter only suspected that they were dealing with criminal property once they had begun to handle the property; or

(3) after the fact, if there was a reasonable excuse.[71]

2.75 If a disclosure is made during or after the transaction has taken place, the disclosure must be made on the reporter's own initiative and as soon as is practicable after the knowledge or suspicion arose.[72]

2.76 Whilst the Secretary of State has power to prescribe the form and manner in which a disclosure is made, this power has not been exercised.[73] However in practice, authorised disclosures seeking consent are made by the reporter submitting a SAR to the UKFIU. If consent to proceed is sought, the reporter must tick the relevant box on the suspicious activity reporting form.

2.77 We briefly referred to DAML SARs and DATF SARs earlier in this chapter. These terms arise from changes made by the UKFIU in 2016. The UKFIU now employ the terms "Defence Against Money Laundering" or "Defence Against Terrorism Financing" as an alternative to the statutory concept of "consent". This was intended to educate reporters, avoid misinterpretation of the term consent and improve the quality of submissions.[74] In the context of the money laundering offences, seeking "consent" is now referred to as seeking a "Defence Against Money Laundering" (DAML). The report that is lodged is referred to as a "DAML SAR".

2.78 Whilst in practice the terms used to describe the consent process have developed, no amendment has been made to the legislation to reflect this change in terminology. As the legislation continues to employ the word "consent", the statutory language will be adopted throughout this paper for clarity.

Consent

2.79 "Appropriate consent" means, in effect, consent to do a prohibited act following an authorised disclosure. In other words, the UKFIU is able to grant permission to do one of the actions otherwise criminalised in the principal money laundering offences (subsections 327 to 329 of POCA) if the reporter makes an authorised disclosure detailing their suspicion.

2.80 For example, if a bank was suspicious that a client's instruction to transfer funds from the UK to an overseas bank account involved criminal property, they should disclose their suspicion to the UK Financial Intelligence Unit. If consent was granted, the transaction could be completed and no criminal offence under section 327 of the Proceeds of Crime Act 2002 would have been committed by the bank or any member of the bank. If the bank chose to execute the transaction without making an authorised

---

71 Proceeds of Crime Act 2002, ss 327(2)(a), 328(2)(a), 329(2)(a) and 338.

72 Proceeds of Crime Act 2002, s 338(3)(c).

73 Proceeds of Crime Act 2002, s 339.

74 National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2017,* p 4

disclosure, they would be at risk of personal criminal liability if the property in question was the proceeds of criminal activity.

2.81 There are three ways in which appropriate consent can be obtained.

(1) **Explicit consent**: Consent can be given by a nominated officer, constable or customs officer. In practice, consent decisions are made by officers in the UKFIU in conjunction with law enforcement agencies.[75]

(2) **Deemed consent on expiry of the notice period**: If having made an authorised disclosure, a reporter does not receive notification of refusal within the statutory notice period, they are to be treated as having consent to proceed. This is known in practice as "deemed consent". The notice period is the period of seven working days starting with the first working day after the person makes the disclosure.[76]

(3) **Deemed consent on expiry of the moratorium period**: Where consent is refused within the seven-day notice period, a moratorium period is triggered lasting for a further 31 calendar days in which the reporter must not act. At the end of this period, the reporter is treated as if they have been given consent to proceed. This allows law enforcement agencies time to take further action such as seeking to restrain assets or seize property. This period can now be further extended on application to the court as will be explained below.

2.82 Consent has a dual function. First, it provides an opportunity for law enforcement agencies to consider and take action to restrain criminal assets or otherwise disrupt criminal activity. Secondly, it protects those who may unavoidably come into contact with criminal property in the course of their employment or professional duties by providing them with an exemption for their conduct which would otherwise be criminal.[77]

2.83 Appropriate consent does not cleanse the entire transaction and/or decriminalise the proceeds of crime. Reporters remain liable for any involvement in the original offence which yielded the criminal proceeds.[78] The NCA state in guidance to reporters that consent does not imply approval of their proposed course of action. Neither does it protect a reporter from any regulatory offences or breach of professional duties arising from their conduct.[79] Appropriate consent signifies that either (a) action will not be taken by law enforcement agencies, (b) that law enforcement agencies do not require any further time in which to investigate or restrain assets or (c) a tactical decision has been taken to watch and wait.

---

[75] A nominated officer must not give the appropriate consent to the doing of a prohibited act unless he or she has made a disclosure to the NCA and has received consent from the NCA (or deemed consent). See Proceeds of Crime Act 2002, s 336.

[76] Proceeds of Crime Act 2002, s 335.

[77] National Crime Agency, *Requests for a defence under POCA and TACT ('Consent')* (May 2016), paras 1.2 to 3. See also *Shah v HSBC Private bank (UK) Ltd* [2012] EWHC 1283 (QB).

[78] *JSC BTA Bank v Ablyazov* [2009] EWCA Civ 1124, [2010] 1 WLR 976.

[79] National Crime Agency, *Requests for a defence under POCA and TACT ('Consent')* (May 2016). See also Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulations 86 and 87.

TIPPING OFF

2.84 If a bank employee was to inform the subject of an investigation that5 a SAR had been submitted to the authorities, this could seriously affect the outcome of any investigation. It may also place the reporter in jeopardy if only a small circle of people could have known about the transaction or provided particular matters of personal information. Whilst certain disclosures are permitted, others are prohibited if they risk "tipping-off" a suspect in a criminal investigation.

2.85 Under section 333A of POCA, it is an offence to disclose:

(1) the fact that a disclosure (a suspicious activity report) under Part 7 of the Proceeds of Crime Act 2002 has been made; or

(2) that an investigation into allegations of a money laundering offence is being contemplated or is being carried out.

2.86 In addition, the following two conditions need to be satisfied:

(1) the disclosure must be likely to prejudice any investigation; and

(2) the information on which the disclosure is based must have come to the person in the course of business in the regulated sector.[80]

2.87 Some types of disclosure are permitted under the Act and where these apply, no offence will be committed.[81] For example, banks are permitted to share information in specific circumstances which will be outlined below.

2.88 The maximum penalty for tipping off on summary conviction is imprisonment for a term not exceeding three months, or an unlimited fine or both. On conviction on indictment, the maximum penalty is imprisonment for a term not exceeding two years, or a fine, or both.

Exemptions from tipping off

2.89 Under Section 333D, the following actions are exempt from the tipping off provisions and act as a safety net:[82]

(1) **Required disclosure to a supervisory authority**: Disclosures made by a person to his or her "supervisory authority" by virtue of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 in the limited circumstances and for the purposes specified in section 333D;

(2) **Disclosure made in relation to an application to extend the moratorium period**: If a disclosure is made in the context of proceedings under section 336A

---

80 Proceeds of Crime Act 2002, s 333A.

81 Proceeds of Crime Act 2002, s 333B (disclosures within an undertaking or group), s 333C (permitted disclosures between institutions) and 333D (other permitted disclosures).

82 *Millington and Sutherland Williams on the Proceeds of Crime* (5th Edition, 2018) at para. 21.92.

of Proceeds of Crime Act 2002, the tipping off provisions are disapplied. A Crown Court judge can extend the moratorium period if there is an investigation ongoing which requires further time and is being conducted diligently;

(3) **Disclosures permitted by voluntary information sharing provisions (partially in force):**[83] This exemption will cover voluntary disclosures made in good faith by virtue of section 339ZB of the Proceeds of Crime Act 2002. Section 339ZB permits the regulated sector to share information in specified circumstances if it will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.

(4) **Law enforcement disclosures**: Protection is afforded where a disclosure is for one of the following purposes:

(a) the detection, investigation or prosecution of a criminal offence (whether in the United Kingdom or elsewhere);

(b) an investigation under POCA; or

(c) the enforcement of any order of a court under POCA.

(5) **Legal advice:**[84] Where a professional legal adviser or a relevant professional adviser makes a disclosure (a) which is to the adviser's client, and (b) is made for the purpose of dissuading the client from engaging in conduct amounting to an offence.

(6) **Lack of knowledge or suspicion**: If the person does not know or suspect that the disclosure is likely to prejudice any investigation.[85]

Issues arising from tipping off

2.90 Electronic processes by which modern financial transactions are conducted have created practical difficulties with the tipping off provisions. There is a commercial need and an increasing expectation by bank customers for payments to be made quickly. In banking, payment involves the transfer of monetary value from payer to payee. Whilst 'money' traditionally refers to physical coins and banknotes, in a modern banking world the transfers are of value not of physical property. Cranston has highlighted the commercial need for swift and efficient means of transferring monetary value which has led to the re-conceptualisation of money as something other than notes and coins.[86]

2.91 Electronic funds transfers are now commonplace and can take place rapidly. Electronic bank-to-bank technology enables individuals and organisations to make and receive

---

83 As inserted by Criminal Finances Act 2017, s 11. This provision is only partially in force. s.11 came into force on April 27, 2017 as 2017 c.22 s.58(6)(d) for the limited purpose of enabling the exercise of any power to make provision by subordinate legislation; October 31, 2017 for the purpose specified in SI 2017 No 991 reg.2(b); October 31, 2017 for the purpose specified in SI 2017 No 1028 reg.2(a); not yet in force otherwise.

84 Proceeds of Crime Act, s 333D(2).

85 Proceeds of Crime Act 2002, s 333D(3), and (4).

86 R Cranston, E Avgouleas, K van Zwieten, C Hare, T van Sante, *Principles of Banking Law* (3rd Edition, 2017) at p 363.

fast and efficient payments. Electronic funds transfers take two basic forms: a push (or credit) transfer and a pull (or debit) transfer. There are three principal mechanisms for electronic funds transfers:

(1) Bankers' Automated Clearing Services ("BACS") for medium sized credit transfers and direct debits;

(2) Clearing House Automated Payments System ("CHAPS") for large sterling denominated credit transfers; and

(3) Faster Payments Scheme Limited ("Faster Payments").

2.92 CHAPS offers the facility to make same-day payments within the UK. The CHAPS payment system is used by financial institutions, companies and individuals for high value and time-sensitive payments. For example, solicitors and conveyancers are frequent users of CHAPS to complete housing and other property transactions. Individuals may also use CHAPS to complete a property purchase or to buy a car. There is no upper limit on the value of the transaction and CHAPS is frequently used for high value transactions.[87]

2.93 BACS runs the Direct Debit scheme in the UK which is used to schedule regular payments. It also administers the credit scheme which is used to pay salaries and settle invoices from suppliers. The BACS system deals in advance payments which must be paid on a specified date in the future.[88]

2.94 The most recently adopted payment scheme in the UK is Faster Payments Scheme Limited owned by its members. Faster Payments launched in 2008. It is a real-time payment system that enables virtually instantaneous electronic transfers of funds (mobile, internet, telephone and standing order) to be made at any time of the day or night, seven days a week.[89] The transaction limit for individual payments is currently set at £250,000, although banks may set their own limits. The number of real-time and same-day transactions is increasing rapidly. In March 2018, Faster Payments processed 158.3 million payments amounting to a total of £136 billion.[90]

2.95 Given that customers expect to make real-time transactions and need to make time sensitive payments, banks are placed in considerable difficulty when transactions cannot be completed the same day and, because of tipping off, they cannot explain the reason for delay to their customer. A bank's perceived failure to execute the client's instructions, in the absence of information can lead to litigation in the civil courts. In *K Ltd v National Westminster Bank plc,*[91] the customer argued that the bank was in breach of contract by failing to make a payment and applied for an interim injunction. The Court held that the bank would have no defence to a charge under section 328 of the

---

87 www.bankofengland.co.uk/payment-and-settlement/chaps (last accessed on 16 April 2018).

88 www.bacs.co.uk/pages/home.aspx (last accessed on 16 April 2018).

89 Committee on Payments and Market Infrastructures, *Fast payments – Enhancing the Speed and Availability of Retail Payments* (Basle, Bank for International Settlements, 2016) 22.

90 www.fasterpayments.org.uk (last accessed on 16 April 2018).

91 [2006] EWCA Civ 1039; [2007] 1 WLR 311.

Proceeds of Crime Act 2002 were it to execute its client's instructions to avoid a breach of contract. As the law made it a criminal offence in the circumstances to honour the customer's mandate, there could be no breach of contract.[92]

2.96 The difficulties created by these provisions for banks was also considered in *Shah v HSBC Private Bank (UK) Limited*.[93] The Court of Appeal confirmed that a bank was not obliged to provide its customer with details of a disclosure. The bank had an obligation to withhold such information if it amounted to a tipping off offence.

2.97 Customers may refer a case to the Financial Ombudsman Service (FOS) after completing the internal complaints process of their bank. If the bank rejects the customer's complaint on the basis that they acted in compliance with their legal and regulatory obligations, or takes longer than eight weeks to reach a decision, a customer can still pursue a FOS complaint. As the bank is unable to disclose the fact that it has made an authorised disclosure and submitted a SAR, it may be unable properly to defend a complaint due to the risk of tipping off the customer.

2.98 In addition to civil litigation or FOS complaints, branch and helpdesk staff encounter the practical problem of managing a customer whose account is blocked. One of the largest reporting banks raised with us real concerns about the safety of their staff who stand between the transaction unit and the customer. It was not uncommon for staff to encounter threats of violence or suicide. At the very least, staff encounter pleas for money to be released so that essential bills can be paid and family life can resume. It can be very hard for staff to deal with pleas for help in the face of financial hardship.

2.99 Banks may also wish to terminate the relationship with their client once there are grounds to suspect money laundering. Consent would be required to pay back any funds to the customer. The closure of an account may alert a criminal that they are being investigated. A tension exists between law enforcement agencies who may want the account to remain open whilst the bank does not want to continue its relationship with the customer in the face of such risk.

INFORMATION SHARING

2.100 The sharing of information between law enforcement agencies and the private sector is an essential part of the proper functioning of the anti-money laundering regime. We discuss this in detail later in this Paper.

Joint Money Laundering Intelligence Taskforce (JMLIT)

2.101 The Joint Money Laundering Intelligence Taskforce ("JMLIT") is a partnership between law enforcement agencies and the financial sector which provides a forum to share information in relation to "high-end" money laundering. The legal gateway which allows the flow of information between the private sector and law enforcement agencies is provided by section 7 of the Crime and Courts Act 2013. This is a broad provision

---

92 [2006] EWCA Civ 1039 at [9]; [2007] 1 WLR 311.

93 [2010] EWCA Civ 31; [2010] 3 All E.R. 477.

allowing any person to disclose information to the NCA if the disclosure is made for the purposes of the exercise of any NCA function.

2.102 Private sector data on financial transactions and law enforcement agencies intelligence on crime can be a powerful combination. When this data has been shared, for example through JMLIT, there have been positive outcomes for both sectors.[94]

2.103 In addition to JMLIT, there are other information sharing arrangements in place such as the Financial Crime Information Network (FIN-NET) and the Shared Intelligence Service (SIS). The Financial Crime Information Network (FIN-NET) is an organisation that operates under the umbrella of the FCA and allows the sharing of information between law enforcement agencies and regulators on specific individuals and entities.[95]

Information sharing under the Criminal Finances Act 2017

2.104 The Criminal Finances Act 2017 introduced new information sharing provisions, intended to assist banks and other businesses to communicate with each other when there is a suspicion of money laundering or terrorism financing. At the time of writing, these provisions are not fully in force.[96] The provisions will offer a second legal gateway which supplements section 7 of the Crime and Courts Act 2013 by allowing bank-to-bank sharing in order to encourage better use of public and private sector resources to combat money laundering.[97] These provisions run in parallel with the existing SARs regime.

2.105 The Act allows for regulated bodies to share information with each other, where they have notified the NCA that they suspect activity is related to money laundering. This measure enables the submission of joint disclosure reports, which bring together information from multiple reporters into a single SAR that provides the whole picture to law enforcement agencies. These "Super SARs" may provide better quality intelligence to law enforcement agencies by combining data from more than one source.

2.106 The provisions allow either a bank or business or the NCA to begin the information sharing process where the disclosure of the information will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering. The legislation is being implemented in phases with credit and financial institutions

---

94 See http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit (last accessed on 27 April 2018).

95 https://www.gov.uk/government/consultations/call-for-information-anti-money-laundering-supervisory-regime/call-for-information-anti-money-laundering-supervisory-regime accessed on 30 April 2018.

96 Proceeds of Crime Act 2002, ss 339ZB-339ZG inserted by Criminal Finances Act 2017, s 11. These provisions are only in force to a limited extent. Criminal Finances Act 2017, s 11 came into force on April 27, 2017 for the limited purpose of enabling the exercise of any power to make provision by subordinate legislation; October 31, 2017 for the purpose specified in SI 2017 No 991 reg.2(b); October 31, 2017 for the purpose specified in SI 2017 No 1028 reg 2(a); not yet in force otherwise) inserted by criminal Finances Act 2017. Terrorism Act 2000, ss 21CA to 21CF inserted by Criminal Finances Act 2017 s 36. These provisions are only in force to a limited extent. Section 36 came into force on April 27, 2017 for the limited purpose of enabling the exercise of any power to make provision by subordinate legislation; October 31, 2017 for purposes specified in SI 2017 No 991 reg 2(f); October 31, 2017 for the purpose specified in SI 2017 No 1028 reg 2(b); not yet in force otherwise.

97 Explanatory Notes to the Criminal Finances Act 2017, para 21.

being the first to be permitted to share information. The legislation does make provision for this to extend to professional advisers in the future.[98]

2.107 Sharing information under the new provisions is voluntary and does not displace the legal obligation to submit a SAR where there is a suspicion of money laundering. Statutory protection is provided against breach of confidence, any other restriction on disclosure and tipping off where information is shared in good faith.[99] Those sharing information must still take steps to comply with their data protection obligations.

2.108 There are two types of information sharing provided for under sections 339ZB to 339ZG of the Proceeds of Crime Act 2002:

(1) where a bank (or business) wishes to share information with another bank or business; and

(2) where the NCA requests a bank or business to share information with other banks/businesses.

REGULATING BUSINESSES AND PROFESSIONALS

The Money Laundering Regulations 2017

2.109 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("The Money Laundering Regulations 2017")[100] impose additional obligations on those in the regulated sector. They implement the Fourth Money Laundering Directive ("4AMLD") and set out the regulatory obligations imposed on banks and businesses. Generally, businesses are required to undertake risk assessments and develop policies, controls and procedures to mitigate and manage the risks of money laundering and terrorist financing.

2.110 The Regulations impose a responsibility to conduct due diligence checks such as verifying the identity of the customer, the company or the beneficial owner of a company. Where customer due diligence cannot be undertaken, the Regulations provide for the relationship to be terminated and allows any funds to be repaid to the customer where consent to the transaction has been given.[101]

2.111 Businesses are required to undertake enhanced customer due diligence measures where there is a high risk of money laundering and terrorist financing. For example, a complex or unusually large transaction or a transaction which appears to have no apparent economic or legal purpose should be looked at more closely. Enhanced measures may include seeking additional independent, reliable sources to verify

---

98 Home Office Circular: *Criminal Finances Act 2017 – Money Laundering: Sharing of Information within the Regulated Sector Sections 339ZB-339ZG*, para 10.

99 Proceeds of Crime Act 2002, s 339ZF, s 339ZB and para 37, s 2 of Schedule 5 to the Act.

100 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692.

101 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulations 27, 28 and 31.

information or taking additional measures to develop a better understanding the customer and the transaction.[102]

2.112 Simplified customer due diligence measures apply where the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing unless there is reason to doubt the veracity of the information provided.[103]

2.113 There is a requirement that the NCA makes arrangements to provide appropriate feedback on suspicious activity disclosures at least once a year.[104] Personal data obtained in order to comply with obligations under the Money Laundering Regulations 2017 is limited to be being processed for the purposes of preventing money laundering or terrorist financing.

2.114 Breach of a requirement under the Regulations is a criminal offence, although it is not an offence if a person took all reasonable steps and exercised all due diligence to avoid committing an offence. The Court must take into account any relevant guidance when deciding whether a requirement was breached.[105] It is also an offence to prejudice an investigation into such a breach.[106] The maximum penalty for either offence on summary conviction is three months imprisonment, a fine or both. On indictment, the maximum penalty is two years' imprisonment, a fine or both.[107]

Supervisory authorities

2.115 There are 22 accountancy and legal professional body anti-money laundering supervisors in the UK whose responsibility is to ensure that their members act in compliance with their obligations under the Money Laundering Regulations 2017.[108] In addition, there are statutory anti-money laundering supervisors who cover the remaining regulated sector entities, for example the Financial Conduct Authority ("FCA"), Her Majesty's Revenue and Customs ("HMRC") and the Gambling Commission.

2.116 The supervisors and industry bodies provide guidance to their members on the law which is approved by HM Treasury. There are a number of sources of guidance

---

102 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulation 33.

103 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulation 37.

104 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulation 104.

105 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulation 86.

106 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulation 87.

107 Civil penalties are also applicable. See Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692, Regulation 76.

108 Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692.

available. For example, the legal sector AML supervisors have produced guidance for their members[109] as have the accountancy sector.[110]

OPBAS

2.117 In March 2017, the Government announced the creation of the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) which is based within the office of the Financial Conduct Authority. Its aim is to strengthen the anti-money laundering supervisory regime and ensure high standards of supervision. It will focus on the adequacy of anti-money laundering supervision. OPBAS became operational in January 2018.

2.118 OPBAS directly oversees the 22 accountancy and legal professional body AML supervisors in the UK. It will ensure these 22 organisations meet the high standards set out in the Money Laundering Regulations 2017, and has powers to investigate and penalise those that do not.[111] Its specific remit is anti-money laundering regulation and it does not supervise:

(1) members of professional bodies, such as firms, accountants and solicitors, or any other type of business subject to the requirements of the Money Laundering Regulations 2017;

(2) statutory anti-money laundering supervisors such as the Gambling Commission and HM Revenue and Customs; or

(3) activity carried out by professional body supervisors outside the UK.

2.119 In respect of governance, supervisory authorities are required to ensure that advocacy functions are kept functionally separate from disciplinary functions.[112] If a supervisor fails to comply, depending on the nature of the non-compliance, OPBAS can publish a statement of censure or recommend that they be removed as a supervisor.[113]

---

109 http://www.lawsociety.org.uk/policy-campaigns/articles/anti-money-laundering-guidance/ (last accessed on 30 April 2018).

110 https://www.ccab.org.uk/documents/FinalAMLGuidance2018Formattedfinal.pdf (last accessed on 30 April 2018).

111 The professional body supervisors overseen by OPBAS are listed in Schedule 1 to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017 No 692.

112 https://www.fca.org.uk/publication/opbas/opbas-sourcebook.pdf, para 3.4. Regulation 49 of the Money Laundering Regulations 2017 requires a professional body supervisor to make arrangements to ensure that their supervisory functions are exercised independently of any of their other functions which are unrelated to disciplinary matters.

113 The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017, Regulations 16 and 17. The sanction is to recommend removal from Schedule 1 of the Money Laundering Regulations 2017 which designates the relevant supervisory authorities for the purposes of the Money laundering Regulations 2017.

The cost of OPBAS will be shared between the professional body supervisory authorities. In 2017, the Financial Conduct Authority estimated that the cost to be shared between the supervisors is likely to be in the region of £2.25 million per year.[114]

COMMISSION OF INQUIRY INTO STATE CAPTURE

[114] Financial Conduct Authority Policy Statement PS18/9 Recovering the costs of the Office for Professional Body Anti-Money Laundering Supervision: feedback to CP17/35 (April 2018) https://www.fca.org.uk/publication/policy/ps18-09.pdf (last accessed 1 May 2018).

Chapter 3: Terrorism financing

BACKGROUND

3.1 In 2017, Europol reported that there were a total of 142 failed, foiled and completed terror attacks reported by eight EU Member States. Of this figure, 76 of these were reported by the United Kingdom.[1] The majority of terrorist attack plots in the United Kingdom have been planned by British residents.[2] The largest attacks in recent years have been the 7/7 bombings and more recently the May 2017 Manchester Arena bombing. At the time of writing there are approximately 3,000 subjects of interest ("SOIs") who are actively under investigation in relation to terrorism. In addition, there are 20,000 individuals of concern who continue to be monitored by law enforcement agencies.[3]

3.2 Whereas a criminal seeks to legitimise criminal cash and maximise the proceeds of their crime by moving it into the financial system, raising and moving funds is not the primary aim of terrorists. Terrorists are not looking to make long-term profit from funds. Instead, these funds are moved for a specific objective such as deployment in support of terrorist groups.

3.3 Funds can also be applied to the attack itself. Lone actor attacks have increased and have proved ever more difficult to detect. Home-made bombs such as the improvised explosive device ("IED") made by Ahmed Hassan which was planted on a district line tube train in September 2017 can be manufactured at low cost. One of the ingredients for this IED was purchased using a £20 Amazon voucher and obtained through an online financial transaction.[4] Recent terrorist attacks across Europe have demonstrated that the funds required to mount lone actor attacks are small. For example, low-cost terrorist activities include hiring a vehicle to drive into a crowd or purchasing weapons such as knives. These attacks lack sophistication and require little planning. Contemporaneous or recent intelligence is vital in preventing terrorist attacks.

3.4 Terrorist financing activity in the United Kingdom typically involves small amounts of money, that may be legitimate in origin. These funds are raised by UK-based individuals either to send to terrorist groups abroad, to fund their own travel to join terrorist groups, or to fund their own attacks. In some cases, money can be donated directly to a central organisation, network or charity to fund living expenses, training, travel or equipment.

---

1 European Union Agency for Law Enforcement Cooperation (Europol), *EU Terrorism Situation and Trend Report* (TE-SAT) (2017), p 10.

2 HM Treasury and Home Office, *National risk assessment of money laundering and terrorist financing* (October 2017), pp 26 to 27.

3 Interview with NTFIU 2 May 2018.

4 Sentencing remarks of the Hon. Mr Justice Haddon-Cave in R v Hassan, para 20 https://www.judiciary.gov.uk/wp-content/uploads/2018/03/r-vhassan-sentencing.pdf, (last accessed on 18 April 2018).

Low-value transactions intended to raise funds for the purposes of terrorism are difficult to detect within the financial system.[5]

3.5 Recent EU terrorist attacks have been funded by a mix of legitimate and illicit funds. Up to 40% of terrorist plots in Europe are believed to be at least partly financed through crime.[6] For example, the Madrid bombings in 2004 were partly financed by credit card fraud. Whilst the importance of Suspicious Activity Reports ("SARs") is clear, the overall volume of SARs can be problematic in isolating essential intelligence. In relation to the 9/11 attacks on the World Trade Centre in the USA, one of the terrorists had been the subject of a SAR in 2000. Ryder observes that the 9/11 Commission were critical of the US SARs regime: the SAR relating to one of the suicide bombers was one of over 1.2 million such reports filed with the US authorities between 1996 and 2003; a needle in a giant haystack.[7]

3.6 In the aftermath of a terrorist attack, the first 24 to 48 hours are crucial to a successful investigation. Investigators rely on intelligence sharing with banks through the Joint Money Laundering and Intelligence Taskforce ("JMLIT"). There is significant co-operation to provide information quickly allowing investigators to build an intelligence picture. Building a comprehensive financial profile of known individuals is an essential part of the investigative process. Intelligence provided in SARs can help with this. A financial picture will allow investigators access to an attacker's financial associates and other important personal information such as contact details. Combined with other evidence, it provides an essential piece of the investigative jigsaw puzzle. It can be instrumental in understanding whether there will be a secondary attack and tracking down the perpetrators or cell involved.

THE CURRENT LAW

Overview of the Terrorism Act 2000

3.7 The legal framework for the counter-terrorism financing regime is found in Part 2 of the Terrorism Act 2000. It creates a parallel regime to the money laundering provisions in Part 7 of the Proceeds of Crime Act 2002 with some significant differences, which will be examined below. For the purposes of this paper, there are four important subdivisions to consider:

(1) disclosure obligations on the regulated sector where there is a suspicion of terrorist property under sections 19 and 21A of the Terrorism Act 2000;

(2) terrorism financing offences. Part 2 creates offences of fund raising for the purposes of terrorism under section 15 of the Terrorism Act 2000; using or possessing terrorist property under section 16 of the Terrorism Act 2000 (similar to section 329 of the Proceeds of Crime Act 2002); and entering into or becoming concerned in an arrangement in relation to terrorist property under section 17 of

---

5 European Union Agency for Law Enforcement Cooperation (Europol), *EU Terrorism Situation and Trend Report* (TE-SAT) 2017, p 12.

6 Above, p 12.

7 Nicholas Ryder, "A false sense of security? An analysis of legislative approaches towards the prevention of terrorist finance in the United States and the United Kingdom." [2007] *Journal of Business Law,* p 849.

the Terrorism Act 2000 (similar to section 328 of the Proceeds of Crime Act 2002);

(3) exemptions to the terrorism financing offences; as with section 338 of the Proceeds of Crime Act 2002, section 21 of the Terrorism Act 2000 creates an exemption from all of the terrorism financing offences (sections 15 to 18) where an individual makes an authorised disclosure. They must disclose their suspicion or belief that the money or other property is terrorist property and obtain consent from the National Crime Agency ("NCA"); and

(4) tipping off offences for individuals in the regulated sector.

Disclosure of information

3.8 There are two forms of disclosure that a bank or business may make:

(1) **Required disclosure:** which provides intelligence to law enforcement agencies in relation to terrorism financing. Banks and businesses have a duty to report any suspicion they may have that someone is laundering terrorist property or committing any of the terrorist financing offences under sections 15-18 of the Terrorism Act 2000.[8] The failure to lodge a suspicious activity report where the conditions for reporting are met is criminal unless one of the exemptions applies.

(2) **Authorised disclosure ("Arrangements with prior consent"):** A bank official or an employee may intend to complete a financial transaction[9] but before completion, becomes suspicious or forms the belief that the transaction involves terrorist property. If they disclose their suspicion to the NCA and obtain consent to proceed, they will be protected from criminal liability in relation to a terrorism financing offence.[10]

The suspicious activity reporting process: terrorism

3.9 Much of what was discussed in Chapter 2 applies to the administrative process for reporting suspicion of terrorism financing with some small differences. Once a SAR has been submitted to the NCA and uploaded to the ELMER database, terrorism financing related SARs are identified using keyword searches undertaken by staff at the UK Financial Intelligence Unit ("UKFIU") . As outlined above, the authorised disclosure exemption applies to terrorism financing offences as well.[11] The NCA refer to this as a "Defence Against Terrorism Financing" SAR ("DATF SAR"). For example, a mother may use a money transfer company to send £150 to her son in Syria. If staff suspect that the payment may be related to terrorism, they must make an authorised disclosure to the NCA and seek consent before making the transfer. These SARs are referred to the National Terrorist Financial Intelligence Unit ("NTFIU"). This unit is part of the Metropolitan Police Counter Terrorist Command. Although they conduct investigations

---

8 Terrorism Act 2000, s 19.

9 Or enter into a financial arrangement. Terrorism Act 2000, s 21ZA.

10 Terrorism Act 2000, s 21ZA and offences in ss 15 to 18.

11 Terrorism Act 2000, s 21ZA.

in London, they manage relationships with the NCA and the private sector on behalf of other regional units.

3.10 Where consent is sought, a team of financial investigators examine the intelligence provided in SARs. Investigators will consider all available intelligence and make a recommendation on whether or not consent should be granted which will be communicated to the NCA. If the NCA consent to the transaction then it can go ahead. If refused, the bank officials should not continue to act. If they were to do so, they would expose themselves to criminal liability for a terrorism financing offence.

3.11 The principal difference between the process for DAML SARs (those seeking consent to complete a bank transaction or a property purchase for example) and DATF SARs (those seeking consent where it is suspected that the money will fund terrorism) is that whilst the seven-day time limit applies, there is no further moratorium period. In practice this means that either:

(1) consent is granted within the seven-day period and, in our example above, the funds can be sent to Syria; or

(2) consent is refused and the bank should not proceed with the transfer of funds. If they do, they are exposed to criminal liability; or

(3) no decision on consent is received by the expiry of the time limit. In this situation, the bank officials can send the funds if they wish to do so as they have "deemed consent".

3.12 Because of the particular sensitivity of DATF SARs, they are not distributed to all law enforcement agencies in the same way as DAML SARs. They are subject to periodic reviews by the NTFIU every 30 days. After the first 90 days have passed, they are subject to quarterly reviews.[12]

Terrorism

3.13 'Terrorism' is defined broadly by section 1 of Terrorism Act 2000.[13] The definition applies to five specific acts where a person:

(1) uses or threatens serious violence against a person,

(2) causes serious damage to property,

(3) endangers another person's life,

(4) creates a serious risk to the health or safety of the public (or a section of the public), or

(5) performs anaction which is designed seriously to interfere with (or disrupt) an electronic system.

---

12 Interview with UK FIU Staff.

13 As amended by s 34 of the Terrorism Act 2006, and by s 75(2) of the Counter-Terrorism Act 2008.

3.14 The action, or threat of it, must be one that is designed to influence the government, an international governmental organisation, or to intimidate the public (or a section of the public), for the purpose of advancing a political, religious, racial, or ideological cause.

Terrorist property

3.15 Like criminal property, "terrorist property" is defined broadly[14] and includes property to be used for terrorism and proceeds from acts of terrorism:[15] Proceeds of an act of terrorism includes any property which wholly or partly, directly or indirectly, represents the proceeds of an act of terrorism.[16] For example, this definition would cover money obtained from a fraudulent benefit claim to purchase bomb-making equipment. It would also encompass any resources of a proscribed organisation such as money set aside to pay rent or utility bills.[17] Whereas the concept of 'criminal property' for the purposes of POCA 2002 has a mental ingredient (i.e. that the alleged offender knows or suspects that the property constitutes or represents a person's benefit from criminal conduct), the definition of 'terrorist property' does not.

Terrorism offences

3.16 The terrorism financing offences are set out in sections 15 to 18 of the Terrorism Act 2000.

Fund-raising

3.17 Three separate offences are created by section 15 of the Terrorism Act 2000:[18]

(1) inviting another to provide money or property *intending* or *having reasonable cause to suspect* that the property may be used for the purposes of terrorism;[19] or

(2) receiving money or other property *intending* or *having reasonable cause to suspect* that the property may be used for the purposes of terrorism;[20] or

(3) providing money or other property *knowing* or *having reasonable cause to suspect* that the property may be used for the purposes of terrorism.[21]

3.18 The offences within section 15 are the most frequently utilised of all the terrorism financing offences. These offences would catch behaviour such as sending payments to a friend who was intending to fight on behalf of the Islamic State (IS) group. If a person sent £100 to a friend in Turkey, that would not provide reasonable cause to

---

14 Terrorism Act 2000, s 14(1).

15 Explanatory Notes to the Terrorism Act 2000 at [27].

16 Terrorism Act 2000, s 14(2)(a).

17 *Millington and Sutherland Williams on Proceeds of* Crime (5th Edition, 2018) para 23.16.

18 In force, 19 February. 2001 (see SI 2001 No 421).

19 Terrorism Act 2000, s 15(1); By s 15(4), "a reference to the provision of money or other property is a reference to its being given, lent or otherwise made available, whether or not for consideration."

20 Terrorism Act 2000, s 15(2).

21 Terrorism Act 2000, s 15(3).

suspect that the property may be used for the purposes of terrorism. However, if the two friends were connected via social media and the recipient had posted material concerning his ambition to join the fight for an Islamic State, this may well meet the objective test.[22] Text messages, emails and other material may also provide evidence that there was reasonable cause to suspect.

Use and possession of terrorist property

3.19 A person commits an offence contrary to section 16(1)[23] if he or she either:

(1) 'uses' money or other property for the purpose of terrorism; or

(2) possesses property intending, or having reasonable cause to suspect that it may be used for the purposes of terrorism.[24]

Funding arrangements

3.20 It is an offence contrary to section 17[25] if a person:

(1) enters into, or becomes concerned in an arrangement, as a result of which money or other property is made available, or is to be made available to another; and

(2) he or she knows or has reasonable cause to suspect that it will be, or may be, used for the purposes of terrorism.

Insurance payments made in response to terrorist demands

3.21 It is an offence contrary to section 17A[26] for an insurer to pay out under an insurance contract in response to a demand made wholly or partly for the purposes of terrorism. The insurer or the person authorising payment must know or have reasonable cause to suspect that the money or other property has been, or is to be, handed over in response to such a demand. This offence would cover situations where a ransom was demanded by a terrorist group in order to release a hostage.

'Money laundering': Facilitating the retention of terrorist property

3.22 It is an offence contrary to section 18[27] for a person to enter into or to become concerned in an arrangement which facilitates the retention or control of terrorist property, whether by concealment, by removal from the jurisdiction, by transfer to nominees, or in any other way.

---

22 *R v Sally Lane and John Letts* [2018] UKSC 36.

23 In force 19 February 2001 (see SI 2001 No 421).

24 Terrorism Act 2000, s 16(2).

25 In force 19 February 2001 (see SI 2001 No 421).

26 Added into the Terrorism Act 2000 by the Counter-Terrorism and Security Act 2015; in force 12 February 2015.

27 In force 19 February 2001 (see SI 2001 No 421).

Exemptions

3.23 There are three exemptions which apply to all of the terrorism financing offences. The common thread is that the bank or business is co-operating with the police:

(1) **Express Consent:**[28] No offence is committed if a person acts with the express consent of a constable. This would protect informants and ensure covert operations or surveillance could continue.

(2) **Arrangements with prior consent:**[29] No offence will be committed if a person discloses the information he or she has in respect of terrorist property on his or her own initiative as soon as reasonably practicable and obtains consent from the NCA to continue with any transaction or financial arrangement.

(3) **Reasonable Excuse:**[30] No offence will be committed if a person intended to disclose their suspicion to the NCA and there is reasonable excuse for their failure to do so.

3.24 An additional defence applies where a person is charged with laundering terrorist property under section 18 of the Terrorism Act 2000. The offender would need to prove that he or she did not know and had no reasonable cause to suspect that the financial arrangement he or she was involved in related to terrorist property.

Information sharing within the regulated sector

3.25 Following amendments made by the Criminal Finances Act 2017 which are only partially in force at the time of writing, the Terrorism Act 2000 also makes provision for information sharing between banks and businesses. The basic scheme of the provisions is to permit information to be shared between banks and businesses in the regulated sector[31] and law enforcement agencies. The provisions allow for the sharing of information in connection with a suspicion that a person is involved in the commission of a terrorist financing offence, or the identification of terrorist property, its movement or use.[32]

Tipping off in the regulated sector

3.26 As with money laundering, the Terrorism Act 2000 prohibits warning an offender that a bank has disclosed their suspicion of money laundering to the NCA. It is an offence to

---

28 Terrorism Act 2000, s 21.

29 Terrorism Act 2000, s 21ZA.

30 Terrorism Act 2000, s 21(5).

31 "Regulated sector" as defined in Terrorism Act 2000, schedule 3A.

32 Terrorism Act 2000, ss 21CA to CF inserted by Criminal Finances Act 2017, s 36. These provisions are only in force to a limited extent. Section 36 came into force on 27 April, 2017 for the limited purpose of enabling the exercise of any power to make provision by subordinate legislation; 31 October, 2017 for purposes specified in SI 2017 No 991 reg.2(f); 31 October, 2017 for the purpose specified in SI 2017 No 1028 reg.2(b); not yet in force otherwise).

discloses the fact that a SAR has been submitted where it is likely to prejudice any investigation that might be conducted.[33]

3.27 It is also an offence to disclose the fact that an investigation into a terrorism financing offence has commenced or is being contemplated where disclosure is likely to prejudice that investigation. The information on which the disclosure is based must have come to the person in the course of business in the regulated sector.[34]

3.28 The offences are punishable on summary conviction by a term not exceeding three months' imprisonment or a fine, or both. On indictment, the maximum penalty is two years' imprisonment, a fine, or both.[35]

Exemptions

3.29 Internal communications within a bank or business are protected. For example, no offence is committed if the disclosure:

(1) is made by one employee to another within the same organisation;[36]

(2) is made to a supervisory authority, for example a solicitor who contacts the Law Society for advice;[37]

(3) relates to a client/former client of an institution or adviser situated in the EEA or a transaction or service involving them both, and the disclosure is for purpose of preventing an offence under Part III of the Terrorism Act 2000;[38]

(4) is for the purpose of detecting, investigating or prosecuting a criminal offence (within or outside the UK);[39] or

(5) is for the purpose of an investigation or to enforce a court order under the Proceeds of Crime Act 2002 ("POCA").[40]

3.30 Failing to disclose knowledge or a suspicion that a person has committed one of the terrorism financing offences under sections 15 to 18 of the Terrorism Act 2000 is also a criminal offence. This is almost identical to the failure to disclose offences under the money laundering provisions of POCA.[41]

---

33 Terrorism Act 2000, s 21D(1).

34 Terrorism Act 2000, s 21D(3).

35 Terrorism Act 2000, s 21D(4).

36 Terrorism Act 2000, s 21E(2).

37 Terrorism Act 2000, s 21G

38 Terrorism Act 2000, s 21F.

39 Terrorism Act 2000, s 21G.

40 Terrorism Act 2000, s 21G.

41 Peter Binning, "In safe hands? Striking the balance between privacy and security- anti-terrorist finance measures" (2002) 6 *European Human Rights Law Review* 737.

Issues with terrorism financing SARs

3.31 The NTFIU has suggested to the Law Commission that the usefulness of terrorism-related SARs is not necessarily reflected in statistics on charge and prosecution. Whilst convictions for terrorism financing offences under sections 15 to 18 of the Terrorism Act 2000 were less frequent, this did not reflect the overall utility of SARs. There are cases were the outcome is disruption of terrorist activity rather than a prosecution for a terrorism financing offence. For example, a suspected terrorist planning an attack may commit credit card fraud which is flagged and reported as suspicious activity by a bank. Rather than seek further evidence to pursue a prosecution for a terrorism financing offence, the credit card fraud can be prosecuted separately, effectively disrupting any plans for an attack.

3.32 Whilst other criminal activity may be prosecuted instead of a specific terrorism financing charge, the Crown Prosecution Service may take the view that an alternative terrorism offence represents the most appropriate charge. For example, the evidence may equally support a charge of preparation for an act of terrorism.[42] In this way, the original financial connection may be only one part of charging and prosecuting an offender, albeit an important part of the investigative chain.

3.33 The NTFIU expressed to the Law Commission similar concerns to the NCA as to the quality of SARs it is receiving. The NTFIU are under time pressure from two different sources. First, the statutory seven-day period for either granting or refusing consent. Secondly, the general pressure to ensure that terrorism SARs are investigated promptly because of the nature of the risk.

3.34 The NTFIU observed that suspicion is inconsistently applied by reporters. Frequently a very low threshold is adopted by reporters which meant that the intelligence provided is not useful. For example, in the aftermath of recent terror attacks in London in 2017, some banks were submitting DATF SARs to close accounts and pay back customers because they had some fleeting transactional relationship with one of the attackers or had lived in the same street. The current SAR form also made it difficult to get to the heart of the suspicion. The free-text box on the form meant that a muddled and confused account could be submitted without specifying what the grounds for suspicion were.

3.35 In respect of the scope of the suspicious activity reported, the NTFIU noted that the following SARs are generally of little effect or value:

(1) Retrospective SARs are less helpful in terrorism financing cases given the relatively short time period in which attacks were planned. Unsophisticated attacks could be planned and executed in less than six months and often no more than 12 months. Historic information is of little value.

(2) SARs which are submitted solely due to the geographical location of the transaction. For example, SARs which are lodged simply because money is being transferred to a country associated with terrorism without any other ground for suspicion.

[42] Terrorism Act 2006, s 5(1).

(3) SARs triggered by police enquiries are often defensive rather than articulating any independent ground for suspicion. If police made an initial enquiry of a bank which related to John Smith, some banks would submit a SAR on John Smith and seek consent to close his account and transfer funds back to him. There may not be any further objective grounds for suspicion beyond the police's interest. These types of SAR are unlikely to provide any useful information to the NTFIU and the closure of an account may be counter-productive to an investigation. It is often more helpful for accounts to stay open to avoid tipping off an individual that he or she is being investigated. The NTFIU are attempting to deal with this through co-operation with the banks but they expressed concern that they lacked the legal power to keep a bank account open. It may also inhibit enquiries or the circulation of subjects of interest ("SOIs") if the potential consequence is that the offender is alerted.[43]

3.36 Chapter 4 will consider how we measure the effectiveness of the consent regime. We will then consider the most pressing bars to effectiveness and propose potential solutions.

[43] Interview with NTFIU.

Chapter 4: Measuring effectiveness

4.1 Whilst it is acknowledged that the suspicious activity reporting regime can provide crucial intelligence, other impacts cannot be ignored. UK Finance have estimated that there are over 18.6 billion transactions each year in the UK to be monitored for money laundering and terrorist financing. Financial institutions investigate approximately 20 million alerts which are produced by automated response systems calibrated to flag unusual activity.[1]

4.2 Of these 20 million alerts generated annually, we know that the total number of Suspicious Activity Reports ("SARs") received by the UK Financial Intelligence Unit ("UKFIU") between October 2015 and March 2017 was 634,113. Of these reports, 27,471 sought consent where there was a suspicion of money laundering (now referred to as a "Defence Against Money Laundering" ("DAML")) and 422 sought consent where there was a suspicion of terrorism financing (referred to as a "Defence Against Terrorism Financing" ("DATF")).[2] These are the most resource intensive type of SAR for the UKFIU. Each one must be allocated to a case worker and investigated for a decision to be reached on whether the bank transaction should be allowed to proceed or whether law enforcement agencies need further time to investigate.

4.3 The simplest way to evaluate the effectiveness of the consent regime is to calculate the number of consent SARs which are of value to law enforcement agencies. We can do this by looking at the total amount of DAML SARs received by the UKFIU and isolating those where consent was refused. The refusal of consent would indicate that further action by law enforcement agencies was anticipated or in process. This means that there would be a realistic prospect of restraint or seizure within the time limits allowed under the Proceeds of Crime Act 2002.[3] Of the 27,471 DAML SARs during that period, consent was refused in only 1,558 cases (5.67%). Of the 422 DATF SARs, consent was refused in 29 cases (6.87%).

4.4 Of the remaining 26,306 consent SARs (either DAML or DATF), either consent was granted or deemed consent resulted due to the passage of time. Whilst it is possible for consent to be granted where there is an opportunity to seize criminal cash using appropriate powers within the short timescale, it seems safe to infer from these statistics that the vast majority of consent SARs do not lead to restraint or seizure of assets.[4]

4.5 However, it is important to note that the volume of DATF SARs does not appear to be high by comparison to DAML SARs. In addition, following our analysis in Chapter 3, it is less appropriate to analyse the value of a DATF SAR in terms of asset restraint and recovery. Therefore, the remainder of our analysis focusses on DAML SARs.

---

1 Interviews with UK Finance.

2 All statistics in this chapter are taken from National Crime Agency, Suspicious Activity Reports (SARs) Annual Report 2017, p 6 unless otherwise specified.

3 Interview with UKFIU staff.

4 National Crime Agency, Suspicious Activity Reports (SARs) Annual Report 2017 p 6

4.6 If we examine the figures on assets restrained, it does not improve the overall picture on the issue of effectiveness. One of the objectives of the consent regime is to provide law enforcement agencies with time to investigate and seek seizure or restraint of criminal assets. The total value of funds restrained between October 2015 and March 2017 was £35,893,941. It remains unclear how much of this sum has been recovered post-restraint. The total amount of cash seized as a result of a suspicious activity report where consent was sought between October 2015 and March 2017 was £16,183,553. In addition, HMRC indemnified a further £51,039 and recovered £1,784,845. On 19th March 2018, in answer to a question from Desmond Swayne MP, Home Office Minister (Security) Ben Wallace MP stated that approximately £1.6 billion in criminal proceeds had been secured since the passing of the Proceeds of Crime Act 2002 ("POCA").[5]

4.7 The first Asset Recovery Statistical Bulletin was published in 2017 and provided a 5-year data "snapshot" on asset recovery from 2012-2017.[6] In 2016/17, £201 million of the proceeds of crime were collected, representing a 19% increase overall compared to 2011 (£170 million).

4.8 However, restraint and seizure are not the only measures of the effectiveness of SARs. They can provide a range of intelligence which may assist with an investigation. Therefore there are two important caveats to our analysis. First, these statistics do not reveal the measure of the disruption of criminal activity and money laundering by law enforcement agencies as a result of intelligence provided in suspicious activity reports. In 2017, the NCA reported £600 million in disrupted assets.[7] Whilst the assets might not be the subject of restraint proceedings, the flow of criminal funds is stopped and the criminals are forced to regroup or cease activity. Secondly, there remains an absence of data on how SARs are used by law enforcement agencies. Due to the need to protect those who make disclosures, it is not routinely recorded when a SAR leads to investigation or prosecution by the Crown Prosecution Service. This makes it very difficult to assess the value of intelligence provided where it does not translate into the physical recovery of assets.[8] SARs are used to trigger investigations and complement pre-existing investigations. Over 4,800 trained officers from 77 agencies have direct access to the SARs database. In the absence of a centralised record on the use of these SARs, the amount and value of the intelligence generated from these reports is hard to quantify. However, they are routinely used in general criminal investigations, not just in money laundering or terrorism financing investigations. Therefore SARs are an intelligence resource across a wide range of offending.[9]

4.9 Once we remove the DAML SARs from the overall total, we can assume that the remaining SARs were lodged as "required disclosures" under sections 330, 331 and 332 of POCA. As above, the amount and value of the intelligence generated from these

---

5 *Hansard* (HC), 19 March 2018, vol 638, col 25.

6 Home Office, *Asset Recovery Statistical Bulletin 2011/12 – 2016/17 Statistical bulletin 15/17* (September 2017).

7 Interview with UK FIU staff.

8 Interview with CPS Economic Crime Unit Lawyer 20 April 2018. See Home Office Circular 022/2015: *Money laundering: the confidentiality and sensitivity of suspicious activity reports (SARs) and the identity of those who make them* (18th June 2015).

9 Interviews with UK FIU staff.

reports is difficult to quantify without statistical data on their operational use in the investigation and prosecution of crime.

4.10 At EU level, the reporting regime generates millions of suspicious transaction reports annually, however, Europol estimate that a small fraction (around 10%) lead to further investigation. This would appear to be higher than the UK figure of between 5-7%. Notwithstanding this low percentage, within the EU, the UK has the highest number of suspicious activity reports. The UK and the Netherlands alone account for 67% of all reports filed in the EU; the UK accounting for 36% of all reports.[10] The threshold for reporting in the Netherlands is lower than that in the UK; it requires all unusual transactions to be reported and does not require any suspicion. After investigation by the Dutch FIU, an unusual transaction may be declared suspicious and all STRs are forwarded to investigation services.[11] On this basis, a high volume of reports is unsurprising.

4.11 The outlook is not improving. In its most recent annual report, the National Crime Agency highlighted a substantial growth in the total number of SARs. In addition, there was a rise in the number of cases in which consent was sought.[12] The trend emerging is for a year on year increase in the number of suspicious activity reports received.[13]

4.12 The UK's higher level of reporting may, in part, be explained by the UK's status as the largest financial centre in the European Union (EU) and a hub for cross-border banking.[14] It is the second largest economy in the EU behind Germany. It represents the largest share of EU financial services activity accounting for 24% of financial services activity within the EU. Germany follows at 16%, then France. In addition to the size of the UK's financial sector, banking remains the largest contributor of SARs to the UKFIU accounting for 82.85% of the total number of SARs received.[15] The second largest contribution is made by other financial institutions who are responsible for 3.73% of all reports.[16]

4.13 We can test the assumption that the UK volume of reports is due to the size of its financial sector. We can compare the UK to another jurisdiction where the financial sector is of a similar size.[17] Switzerland is the closest comparator. In 2015, banks in

---

10 Europol, *From Suspicion to Action, Converting Financial Intelligence into Greater Operational Impact* (2017) chart 2.

11 Europol, *From Suspicion to Action, Converting Financial Intelligence into Greater Operational Impact* (2017) p 10.

12 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) p 6.

13 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) figures i-ii and p 17.

14 Para. 1.3 of Joint Home Office and HM Treasury *Action Plan for anti-money laundering and counter-terrorist finance* (2016) and Bank of England, *EU Membership and the Bank of England*, October 2015 Chart 1.10 available electronically at https://www.bankofengland.co.uk/-/media/boe/files/speech/2015/eu-membership-and-the-bank-of-england-pdf.pdf (last accessed 4 June 2018).

15 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) p 11.

16 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) p 11.

17 Bank of England, *EU Membership and the Bank of England*, October 2015 (Chart 1.10, 'The Size of the Financial System Excluding Derivatives') available electronically at https://www.bankofengland.co.uk/-

Switzerland filed 2,159 SARs[18] compared to the UK's 634,113 between October 2015 and March 2017.[19] If we compare the number of SARs received based on the size of our economy, we can look to Germany and France as our peers. Germany, whose economy was worth £2.4 trillion in 2014 by comparison to the UK's £1.8 trillion showed a vastly reduced level of SARs to that of the UK. In 2015, 24,054 reports were filed with the Bundeskriminalamt (Germany's Financial Intelligence Unit).[20] France, with an economy of £1.7 trillion, received a much lower number of suspicious transaction reports. In 2016, Tracfin (France's financial intelligence unit) received a higher number of reports than Germany but still a significantly lower number than the UK with 64,815 suspicious transaction reports.[21]

4.14 We can say with certainty that the current volume of reports was not anticipated when Part 7 of the Proceeds of Crime Act 2002 was in its early stages. Donald Toon, Director of Economic Crime at the National Crime Agency, stated in 2016 that the computerised system for processing SARs (ELMER) was at that time processing 381,882 SARs. This was despite it having originally been designed to cope with a much smaller number of around 20,000.[22] It seems clear from this that the current volume of reports was not anticipated.

4.15 The evidence suggests firstly that the volume of reports in the UK is anomalous compared to its peers. Secondly, the volume of assets restrained or seized is not proportionate to the cost of the regime. Thirdly, valuable reports represent a small percentage of the overall total when assessed in the context of asset recovery. Finally, the large volume of SARs creates resourcing issues for the NCA and other law enforcement agencies.

Causes of the large volume of reports

4.16 It is important to consider what is causing such a high volume of reports which are not useful to law enforcement agencies. There appear to be four principal drivers behind the large number of reports:

(1) **A low threshold for criminality**: The effect of the POCA provisions is to set a lower threshold for criminality (and consequently, reporting) than that required by

/media/boe/files/speech/2015/eu-membership-and-the-bank-of-england-pdf.pdf (last accessed 4 June 2018).

18 Federal Department of Justice and Police (FDJP), Federal Office of Police (Fedpol), Report 2015: *Annual Report by the Money Laundering Reporting Office Switzerland, MROS*, April 2016.

19 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) figure i.

20 Bundeskriminalamt, *Annual Report 2015*, p 9 available at https://www.bka.de/SharedDocs/Downloads/EN/Publications/AnnualReportsAndSituationAssessments/FIU/fiuJahresbericht2015Englisch.pdf?_blob=publicationFile&v=2 (last accessed on 7 May 2018).

21 Tracfin, *Annual Report 2016*, p 8 https://www.economie.gouv.fr/files/ang-ra-tracfin-2016.pdf (last accessed on 7 May 2018).

22 House of Commons, Home Affairs Select Committee, Proceeds of Crime, Fifth Report of Session 2016-17, 15th July 2016 available electronically at https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/25/25.pdf at [24] (last accessed 4 June 2018).

either the Financial Action Taskforce ("FATF") recommendations[23] or the Fourth Money Laundering Directive ("4AMLD").[24] This is achieved in two ways:

(a) adopting an "all-crimes" approach; neither FATF nor the 4AMLD require all crimes to be included as predicate money laundering offences. The 4AMLD refers to "criminal activity"; and

(b) setting the threshold for criminality at suspicion. The 4AMLD mandates that only intentional conduct (of the types described in Article 3(a) to (d)) shall be regarded as money laundering. Knowledge, intent or purpose may be inferred from the objective factual circumstances.

As the threshold is comparatively low, this could be a cause of overreporting. Alldridge attributes the disparity in levels of reporting between the UK and other jurisdictions in part to the UK's lower threshold.[25]

(2) **Individual criminal liability**: The low threshold for criminality combined with individual criminal liability incentivises defensive reporting[26]. Individuals in the regulated sector are at risk of personal criminal liability for their actions which includes where they have been negligent in their failure to report. Goldby argues that the objective test applied to disclosure offences for the regulated sector[27] means that risk averse professionals and employees will report rather than risk prosecution for a failure to do so.

(3) **Confusion as to obligations**: The National Crime Agency have observed that frequently reporters misunderstand the consent provisions and lodge unnecessary SARs.[28] Balanced against this, stakeholders with reporting responsibilities expressed frustration that the legislation requires SARs to be lodged where they are bound to be of no practical value or effect. The legislation does not allow for flexibility or judgment to be applied and simply imposes a "hard-coded obligation" to report.[29]

(4) **Suspicion**: A majority of stakeholders expressed the view that suspicion remains ill-defined, unclear and inconsistently applied by banks and businesses. Stakeholders reported a wide spectrum of suspicion in practice ranging from being unable to complete due diligence on a customer, to being concerned, up to a settled suspicion on objective grounds.

---

23 Financial Action Task Force, *'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation'* 2012

24 Fourth Money Laundering Directive 2015/849 Official Journal L141 of 5.6.2015.

25 Peter Alldridge, *What Went Wrong with Money Laundering Law* (1st ed 2016) p 40.

26 Joint Home Office and HM Treasury Action Plan for anti-money laundering and counter-terrorist finance (2016) p 39.

27 Proceeds of Crime Act 2002, ss 330 and 331. See also Miriam Goldby, Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform *Journal of Business Law* [2013] 368.

28 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) p 17

29 Interviews with UK Finance members.

4.17 The following chapters will examine the above issues and other pressing problems with the current regime before considering provisional proposals for reform.

COMMISSION OF INQUIRY INTO STATE CAPTURE

Chapter 5: The "all crimes" approach

5.1 The UK has adopted an "all crimes" approach in its money laundering offences. What is meant by that is that the definition of criminal property is not limited to property derived from particular crimes or even particular categories of crime. Criminal property can be property, as widely defined, from any crime regardless of the seriousness of the offence.[1]

5.2 One consequence of that is in deciding whether to submit a Suspicious Activity Report ("SAR") the officials in the regulated sector need not consider what likely criminal activity led to the property becoming criminal. This has a significant practical advantage as it means that a bank cashier, for example, does not have to decide whether the cash deposit they are being invited to process by the customer comes from the sale of drugs or represents the proceeds of a burglary or a legitimate business which is evading tax. The reporter is never required to identify the original criminal offence from which the money derives. The terrorist financing reporting requires the reporter be suspicious that the money is the product of a terrorism offence or the monies are going to be used in a terrorism offence. Reporters are not required to identify a specific terrorism offence which the monies are linked to and terrorism offences represent a broad category of offences. In addition, statistics show that far fewer defence against terrorist financing reports ("DATF SARs") are received when compared to defence against money laundering ("DAML SARs").[2] Stakeholders have told us that reporters may be unable to say whether they suspect that the predicate offence is terrorist financing. In such instances, where they suspect the monies are the proceeds of a crime they will submit a DAML SAR.

5.3 In adopting this approach, the UK has exceeded the minimum international standards that have been expressed. The Financial Action Task Force ("FATF") has recommended that the crime of money laundering should be applied to all "serious offences", with a view to including the widest range of predicate offences including terrorist financing.[3] Dr Sarah Kebbell, an academic who has conducted research on the anti-money laundering regime and the legal profession, observes that the UK has elected to "gold plate" its anti-money laundering regime, above that required by FATF or EU law.[4]

5.4 The EU has incrementally widened the scope of the concept of criminal activity which ought to be criminalised by virtue of the money laundering directives. Article 3(4) of the Fourth Anti Money Laundering Directive ("4AMLD") defines "criminal activity" by listing

---

1 Proceeds of Crime Act 2002, s 340.

2 National Crime Agency, Suspicious Activity Reports (SARs) Annual Report 2017, figure i. October 2015 to September 2016: 289 DATF SARs and 17,909 DAML SARs.

3 Financial Action Task Force Recommendations, *International standards on combating money laundering and the financing of terrorism and proliferation* (2012), Recommendations 3 and 5.

4 Sarah Kebbell, ""Everyone's looking at nothing" – the legal profession and the disproportionate burden of the Proceeds of Crime Act 2002", [2017] *Criminal Law Review* 741.

specific crimes. This list covers terrorism offences, drug trafficking, organised crime, fraud, corruption and tax offences. It also covers offences which meet a particular penalty threshold.[5] Specifically, this covers offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year. Alternatively, if a member state expresses criminal penalties by way of a minimum threshold for offences in their legal system, then all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months.[6]

"Technical" breaches

5.5 The all crimes approach adopted in the UK has led to some unintended consequences. One has been to place a disproportionate burden upon the legal profession. Minor offences and regulatory breaches identified during commercial transactions can trigger an obligation on the solicitor executing the transaction to make a disclosure. It also potentially exposes the individual and the firm to liability for a substantive money laundering offence. Kebbell's examples from her research include where a client had failed to comply with a tree preservation order, or to obtain an asbestos-related environmental licence. The notional financial savings made by the offender as a result of the failure to comply with these regulations will constitute criminal property under s 340 of the Proceeds of Crime Act 2002. Once the legal professional dealing with that client suspects the existence of criminal property, it triggers the need to report. That will often be in the form of a DAML SAR requiring consent to complete the commercial transaction. [7]

5.6 To take an example, if a property developer were to breach a tree preservation order during construction of a new housing development, it would be liable for a criminal offence. Breach of a tree preservation order is a non-imprisonable offence.[8] A solicitor conducting the commercial transaction for the property developer would, on identifying the breach and therefore having at least suspicion that the property is criminal, have to lodge a SAR, identifying criminal property from the notional saving made to the property developer in breach of such an order.

5.7 Between October 2015 and March 2017, 4,878 of the overall number of SARs were lodged by the legal sector, amounting to just 0.77% of the total number. However, Kebbell notes that in 2014-15, 75.52% of legal sector SARs were seeking consent and were DAML SARs. The evidence suggests that such reports are more likely to be "technical" in nature on the basis that law firms are seeking consent to continue with a transaction rather than declining to act.[9] The legal profession may be more likely to

---

5 Valsamis Mitsilegas and Niovi Vavoula, 'The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law' (*Maastricht Journal of European and Comparative Law,* 2016).

6 Fourth Money Laundering Directive (EU) 2015/849, Article 3 (4)(f).

7 Sarah Kebbell, *""Everyone's looking at nothing" – the legal profession and the disproportionate burden of the Proceeds of Crime Act 2002",* [2017] *Criminal Law Review* 741.

8 Town and Country Planning Act 1990, s 210.

9 Sarah Kebbell, *""*Everyone's looking at nothing" – the legal profession and the disproportionate burden of the Proceeds of Crime Act 2002*"*, [2017] *Criminal Law Review* 741.

adopt a risk-averse approach due in part to their legal training and the professional consequences of failing to make a disclosure.

5.8 Stakeholders expressed the view that when reporters were obliged to submit a SAR where they perceived it to be for technical compliance rather than of substantive value, they felt this was imposing a disproportionate burden on the sector. As the legal profession tended to comply strictly with their obligations, these SARs could be challenging to report as they required a substantial amount of time to prepare where the criminal property was not easily identified. As Kebbell observes, this may have a negative impact on compliance if a perception develops amongst those in the sector that the regime is broken.[10]

"Serious crimes" rather than "all crimes"

5.9 Not all countries adopt an "all crimes" approach to money laundering. Broadly, having regard to the approaches in other jurisdictions, serious crimes could be identified for money laundering purposes in two ways:

(1) all offences that fall within the category of serious offences under national law, where such a list exists (for example a list of offences in a schedule); or

(2) all offences that are punishable by a maximum penalty of more than one years' imprisonment.[11]

5.10 For example, in the USA, money laundering is criminalised where it relates to specified unlawful activity and the "specified" offences are ones that are listed in statute.[12] Germany also adopts a "serious crimes" approach listing specific serious criminal offences. German law also includes offences which are punishable with at least one years' imprisonment as serious offences.

5.11 There are at least two existing examples in domestic law where serious criminal offences have been classified and listed in a schedule. Schedule 1 of the Serious Crime Act 2007 (eligibility offences for Serious Crime Prevention Orders) and Schedule 2 of the Proceeds of Crime Act 2002 (criminal lifestyle offences for the purposes of confiscation). Both could provide a starting point for adopting a serious crimes approach should that be desirable.

5.12 However, there are problems with such an approach. First it would have to be agreed which of the thousands of offences that exist in UK law would feature. This is particularly problematic given that different offences exist within England and Wales, Scotland and Northern Ireland and thus a serious offences approach could lead to geographical inconsistencies. Secondly, any such schedule of serious offences would need to be regularly re-assessed and up-dated. There is a risk of relevant criminality being omitted.

---

10 Sarah Kebbell, ""Everyone's looking at nothing" – the legal profession and the disproportionate burden of the Proceeds of Crime Act 2002", [2017] *Criminal Law Review* 741.

11 Financial Action Task Force Recommendations, International standards on combating money laundering and the financing of terrorism and proliferation (2012), Recommendation 3 and Interpretative Note to Recommendation 3.

12 Specified Unlawful Activity 18 USC § 1956(c)(7) as cited in18 US Code § 1956 - Laundering of monetary Instruments.

In addition, further legislative amendment would be necessary if more offences were to be included in the future. Given the pace of change in anti-money laundering, this is highly likely. In addition, it would still require an additional level of scrutiny by reporters and would increase the work involved in drafting a SAR.

5.13 There is an attraction in adopting the simpler approach of a threshold based on the maximum penalty available for the particular offence. This would avoid the problem of ensuring that any schedule of offences was up-to-date offences in future based on further EU Directives or FATF recommendations. There are, however, problems with this approach too. What level of threshold would be set? Are we confident that the maximum penalties for offences are consistent and that the threshold would not create arbitrary distinctions? In addition, it would still require an additional level of scrutiny by reporters and would increase the work involved in drafting a SAR.

5.14 Any form of "serious crimes" approach may impact adversely on the ability of law enforcement agencies to prosecute money laundering offences. Currently, the prosecution does not need to identify the predicate offence or even the type of offence as long as the money derives from criminal conduct. If they are unable to point to a specific crime, the prosecution can lead evidence to show the circumstances in which the property was handled were such as to give rise to an irresistible inference that it could only be derived from crime.[13] As Bell has highlighted the US prosecutors faced difficulties because the "serious crimes" approach that has been adopted required them to prove that at least some of the funds were the proceeds of "specified unlawful activity". This can prove to be a barrier to successful prosecutions.[14]

5.15 In our preliminary discussions, stakeholders expressed concerns about moving away from an "all-crimes" approach. Some stakeholders were concerned that a serious crimes approach would complicate an increasingly burdensome regime. Whilst those in the legal sector were less concerned about the obligation that would arise to identify the predicate crime, financial sector stakeholders anticipated difficulties with such an approach. They envisaged that it would be challenging for non-lawyers to identify the underlying criminality. Whilst they may suspect that the funds they were dealing with were criminal property, they might find it difficult to identify the predicate crime.

5.16 Some stakeholders were also concerned that a "serious crimes" approach may create two tiers of criminality, diminishing the importance of, for example, environmental crimes or regulatory offences. A "serious crimes" approach would also be likely to result in predominately corporate or commercial crimes such as regulatory offences being excluded from the remit of money laundering. For example, failure of a commercial organisation to prevent bribery is an indictable only offence where the maximum penalty is a fine.[15] Likewise, failure to prevent facilitation of UK tax evasion offences is triable either way, but the maximum penalty is a fine.[16] These offences would both fail the threshold test. Furthermore, there may be significant financial benefit arising from a

---

13 *R v Anwoir* [2008] 2 Cr App R 36, [2009] 1 W.L.R. 9; *R v F* [2009] Crim LR 45, [2010] Crim. L.R. 329; and R v Gillies [2011] EWCA Crim 2140, [2011] Lloyd's Rep. F.C. 606.

14 R E Bell, (2003) "Abolishing the concept of 'predicate offence'", *Journal of Money Laundering Control*, Vol. 6 Issue: 2, pp.137 to 140.

15 Bribery Act 2010, s 7.

16 Criminal Finances Act 2017, s 45.

"technical" case of money laundering. There seems to be little moral justification for allowing some offenders to enjoy the fruits of their crimes and others to be liable to prosecution. Arguably, no criminal should be allowed to enjoy the proceeds of any crime.

5.17 Our provisional view is that adopting a "serious crimes" approach would be problematic and undesirable. It would create unnecessary complexity and could become a barrier to successful prosecutions.

5.18 We would however welcome comments on the merits of other approaches including:

(1) a serious crimes approach, whether based on lists of offences or maximum penalty;

(2) retaining an all crimes approach for the money laundering offences but requiring SARS only in relation to "serious crimes" (to be defined by category and or sentence as discussed above). This could be achieved by extending the reasonable excuse defence to those who do not report, for example, suspected non-imprisonable crimes or those crimes listed on a schedule; or

(3) providing the opportunity to the regulated sector to draw to the attention of the FIU any non-serious cases, whilst maintaining a required disclosure regime for offences on a schedule of serious offences listed in one of the ways identified above.

Consultation Question 1.

5.19 Do consultees agree that we should maintain the "all crimes" approach to money laundering by retaining the existing definition of "criminal conduct" in section 340 of the Proceeds of Crime Act 2002?

5.20 If not, do consultees believe that one of the following approaches would be preferable?

(1) a serious crimes approach, whether based on lists of offences or maximum penalty;

(2) retaining an all crimes approach for the money laundering offences but requiring SARS only in relation to "serious crimes" (to be defined by category and or sentence as discussed above). This could be achieved by extending the reasonable excuse defence to those who do not report, for example, suspected non-imprisonable crimes or those crimes listed on a schedule; or

(3) providing the opportunity to the regulated sector to draw to the attention of the FIU any non-serious cases, whilst maintaining a required disclosure regime for offences on a schedule of serious offences listed in one of the ways identified above.

COMMISSION OF INQUIRY
INTO STATE CAPTURE

Chapter 6: The meaning of suspicion

THE CONCEPT OF SUSPICION

6.1 As discussed in Chapter 2, suspicion is a key concept in the UK anti-money laundering regime. The legislation sets the minimum threshold of the mental element for the offences under the Act at "suspicion".[1] In relation to the offences, suspicion provides the fault element for the principal money laundering offences. The effect of section 340 of the Proceeds of Crime Act 2002 ("POCA") is that once any person, including a reporter in a professional context, suspects that property is criminal property, the person is liable if they undertake one of the acts prohibited in sections 327 to 329. This is subject to the requirement that the property in question must in fact be the proceeds of crime; there is no conviction on suspicion alone.[2] A reporter must decide whether to make an authorised disclosure and seek appropriate consent to avoid committing a criminal offence.[3] The penalties are severe with maximum sentences of 14 years' imprisonment.

6.2 The test of suspicion is also relevant in providing the threshold for those in the reporting sector to file a suspicious activity report ("SAR").[4] Sections 330 to 332 of POCA require disclosure where a reporter suspects that a person is engaged in money laundering.[5] That obligation is also backed by criminal sanction.

6.3 Despite its significance in both contexts within Part 7, the term "suspicion" is not defined in the 2002 Act. Nor is it defined in either the Financial Action Task Force ("FATF") Recommendations or the Fourth Money Laundering Directive ("4AMLD")[6] which the Act seeks to implement. It has been left to the courts to interpret this and other suspicion-based tests.

6.4 In practice, understanding what suspicion means is crucial for those working in professions in which their duties create a risk they will be dealing with criminal property. If the concept of suspicion is ill-defined, and/or ill-understood, it:

(1) increases the risk that those working in the sector will commit offences by laundering or failing to report; and,

---

1 Proceeds of Crime Act 2002, ss 327 to 329 and 340.

2 *R v Montila* [2004] UKHL 50; [2004] 1 WLR 3141. See also *R v El Kurd* [2001] Crim LR 234 and *R v Anwoir* [2008] 2 Cr App R 36; [2008] EWCA 1354.

3 Proceeds of Crime Act 2002, ss 327(2), 328(2) and 329(2). The Terrorism Act 2000 uses the threshold of "reasonable cause to suspect" for terrorism financing offences in ss 15 to 18.

4 Proceeds of Crime Act, ss 330 to 332.

5 The Terrorism Act 2000 uses the threshold of suspicion for reporting obligations, see for example s 21ZA arrangements with prior consent.

6 Directive 2015/849/EC on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

(2) renders it more likely that unnecessary SARS are made which the NCA has to process: SARs which provide low-value intelligence or defensive SARs in the absence of any real suspicion.

6.5 Given the significance of the concept of suspicion in Part 7 of POCA, this Chapter is the first of three in which we conduct a detailed examination of suspicion, its meaning and application in the context of the consent regime. In the following chapters we will consider:

(1) the concept of suspicion, its position within the hierarchy of fault thresholds and its application in an investigative context;

(2) its application in the context of the money laundering offences and the challenges that arise from using suspicion as a threshold for criminality;

(3) its application in the context of the disclosure offences and the implications of the current law for those with reporting obligations;

6.6 In Chapter 9, we consider the case for reforming the current law based on our analysis in the preceding chapters. We will go on to look at various measures that may improve the quality of reporting, reduce low value intelligence reports and contribute to the overall effectiveness of the disclosure regime.

Concerns about suspicion

6.7 The concern about the lack of clarity in the definition of the concept of suspicion has been recognised to be a problem for some time. In 2006, the threshold of suspicion and its impact on the volume of reporting were already the subject of discussion. In March of 2006, Sir Stephen Lander issued his report following a Serious Organised Crime Agency (SOCA: a forerunner of the NCA) review on SARs in his capacity as Chairman. In his report, he stated that SOCA had sought to make its own judgement about the threshold of suspicion given its concern about "reporting volumes":

> In passing the Terrorism Act 2000 and the Proceeds of Crime Act 2002, Parliament determined to set wide definitions of terrorist and criminal property and significant penalties for money laundering, and to retain a low threshold for disclosures, involving "suspicion", not "knowledge" or "belief". The consequence appears to have been the significant growth in reporting already noted. Two conclusions follow:
>
> First, it would be improper for SOCA as the FIU to seek, against some concern about reporting volumes, to insert its judgement about the threshold for suspicion in place of the duty to make that judgement laid on the reporters by Parliament. In any event, it is self-evident that SOCA would never be better qualified to determine what is suspicious in the context of the reporters' business than the reporters themselves.
>
> Second, it could be argued that in inviting Parliament to establish the regime set out in TA Part 3 and POCA Part 7, Government was accepting the responsibility for ensuring that the resulting volumes of information were handled effectively.
>
> It would be inappropriate, given current legislation, for SOCA as the FIU, or Government more generally, to seek to suppress the overall number of SARs. In short, the correct Government position on numbers of SARs should be volume neutral. In

practice, as already noted in Part III of this report, the current suspicion based approach has been delivering operational benefits to law enforcement agencies, and there are thus grounds for believing that the arrangements are not fundamentally flawed. This does not, of course, mean that reporters should be released from the obligation to distinguish effectively between the unusual and the truly suspicious, nor that the regime would be well served by the removal of the due diligence arrangements put in place by many to make that distinction.[7]

6.8 Sir Stephen Lander also observed that, in 2006, UK volumes of SARs were not beyond the range reported in some other comparable jurisdictions. As we discussed in previous Chapters, that is no longer the case. It is clear from this report that concerns regarding the threshold for reporting and its impact on volume were evident as early as four years after POCA came into force in 2002.

6.9 These concerns have not abated. In 2015, the Home Office's Call for Information[8] on the operation of the SARS regime revealed that those in the reporting sector were concerned as to the phrasing of the requirement to report suspicious transactions as set out in POCA:

> The reporting sector has concerns regarding the phrasing of the requirement to report suspicious transactions, as set out in POCA. This concern, and the penalties for failure to report, drive a significant level of defensive reporting, where reports are made more because of concerns regarding a failure to comply with POCA than because of genuine suspicion. This places a burden on the regime, and detracts from a focus on serious and organised crime. The Government is committed to taking action to recognise and address this concern.[9]

6.10 This may increase the volume of both authorised and required disclosures to the NCA. As we observed in Chapter 2, authorised disclosures are resource-intensive. Poor quality or unfounded disclosures divert resources and attention away from investigating and tackling serious and organised crime. The submission of reports of low intelligence value creates what Goldby has described as 'noise' which serves to distract the attention of law enforcement agencies from the most serious or urgent cases.[10] It must be noted that there is a distinction in this regard between money laundering disclosures and terrorism financing disclosures. The number of SARs in recent years where a defence against terrorist financing (DATF) had been requested was low by comparison with those where a defence against money laundering had been requested.[11] This suggests that the same issue of high volume reporting does not appear to arise in

---

7 Sir Stephen Lander, "Review of the Suspicious Activity Reports Regime" (The SARs Review) (March 2006), pp 53 to 54.

8 Annex B: Findings from the Call for Information on the Suspicious Activity Reports (SARs) Regime of the Joint Home Office and HM Treasury Action Plan for anti-money laundering and counter-terrorist finance (2016).

9 Annex B: Findings from the Call for Information on the Suspicious Activity Reports (SARs) Regime of the Joint Home Office and HM Treasury Action Plan for anti-money laundering and counter-terrorist finance (2016) p 39.

10 Miriam Goldby, Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform. Journal of Business Law (2013) 367 at 382.

11 National Crime Agency, Suspicious Activity Reports Annual Report (2017) figure i.

respect of terrorism financing. However, as we outlined in Chapter 3, there are concerns regarding the quality of reports submitted.

6.11 Given the concerns outlined above, in the next part of this chapter, we will consider why suspicion has been adopted as the threshold for making disclosures. Whilst the 4AMLD sets the minimum threshold for reporting at suspicion or reasonable grounds to suspect, it does not make similar provision for money laundering offences.

Why are the thresholds set at the level of suspicion?

Reporting money laundering or terrorist financing

6.12 The UK's freedom to decide the threshold which triggers an obligation on a person to report money laundering or terrorist financing is circumscribed by international standards and European law. Recommendation 20 of the FATF Recommendations requires Members to impose a reporting obligation on financial institutions where they suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing.[12]

6.13 Article 33 of the 4AMLD states that:

> Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly: (a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing…

6.14 The terms "knows, suspects or has reasonable grounds to suspect" used in both FATF recommendation 20 and Article 33 of the 4AMLD are mirrored in sections 330 and 331 of the Proceeds of Crime Act 2002.[13] Disclosure is required regardless of whether the reporter intends to deal with the criminal property in any way prohibited under the principal money laundering offences.[14] However, where the reporter wishes to transfer or move property in a manner prohibited under the Act, they will make an authorised disclosure and seek appropriate consent in order to benefit from the statutory exemption and avoid committing that principal money laundering offence.[15]

6.15 Suspicion sets a low threshold for these disclosure offences. A reporter who fails to report is committing a crime. That obligation to perform an investigative function backed by criminal sanction is unusual. In one sense, suspicion renders it a very onerous obligation since it requires reporters to be vigilant and report in a high volume of cases. In another sense, since the threshold is low it could be argued to impose a limited burden on the reporter since there is no need to enquire too closely: it requires only

---

12 Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation' 2012.

13 Proceeds of Crime Act 2002, s 332 covers nominated officers outside the regulated sector and requires a disclosure under section 332 where a nominated officer knows or suspects that a person is engaged in money laundering. Reasonable grounds for suspicion is absent from this provision.

14 Proceeds of Crime Act, ss 327 to 329.

15 Proceeds of Crime Act 2002, ss 327(2), 328(2), 329(2) and 338.

minimal effort from reporters. This could be said to recognise the burden of the disclosure regime on the reporter.

Criminal offences

6.16 The FATF Recommendations do not specify the fault threshold for money laundering or terrorist financing offences. However, the interpretative note to Recommendation 3, uses the terms "intent" and "knowledge". The note states that countries should ensure:

> The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances. [16]

6.17 The 4AMLD states in Article 1 that Member States shall ensure that money laundering and terrorist financing are prohibited.[17] The Directive sets out the conduct which, when committed intentionally, shall constitute money laundering:[18]

> For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:
>
> (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
>
> (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
>
> (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
>
> (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

6.18 The requirement is therefore for knowledge of the criminal nature of the property and an intent to deal with it in a proscribed way.

6.19 While the 4AMLD sets the threshold at knowledge, the UK threshold is far below this. The mental fault element adopted in the POCA offences is suspicion. That has been described as "a remarkably low threshold for a criminal offence,"[19] particularly one carrying 14 years as the maximum sentence. However, requiring only a suspicion that

---

16 Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation' 2012, Recommendation 3 and Interpretative Note to recommendation 3, para 7.

17 Article 1(2) of the Fourth Money Laundering Directive (EU) 2015/89, OJ L 141, 5.6.2015, p. 73 to 117.

18 Article 1(3) of the Fourth Money Laundering Directive (EU) 2015/89, OJ L 141, 5.6.2015, p. 73 to 117.

19 Smith, Hogan, and Ormerod's Criminal Law (2018), para 3.2.8 and [2007] Crim LR 77.

property is criminal property may be advantageous to law enforcement agencies. It provides a greater opportunity to monitor, investigate or disrupt criminal activity at an early stage. We will consider this issue in detail later in this paper. In the next section, we begin to explore the definition of suspicion, and how it sits within the spectrum of criminal law thresholds for fault.

SUSPICION IN CRIMINAL LAW

The ordinary meaning of suspicion

6.20 As we noted above, there is no definition of suspicion in the Proceeds of Crime Act 2002 or the Terrorism Act 2000. Suspicion is considered to be an ordinary word of the English language.[20] In *Brutus v Cozens*,[21], the House of Lords endorsed a general principle of statutory interpretation in criminal law that the meaning of an ordinary word of the English language is not a question of law

6.21 It is therefore helpful to start with the ordinary every day meaning of suspicion. Millington and Sutherland Williams[22] refer to the Oxford English Dictionary definition of "suspect" which offers five alternatives:

(1) an impression of the existence or presence of;

(2) believe tentatively without clear ground;

(3) be inclined to think;

(4) be inclined to mentally accuse; doubt the innocence of; and

(5) doubt the genuineness or truth of a suspected person.

6.22 The Chambers English Dictionary has defined "suspicion" as, "a belief or opinion that is based on very little evidence"; a slight quantity".[23] The Cambridge English Dictionary[24] offers a number of different definitions: "to think likely" or "to think or believe something to be true or probable." In addition, "to think that someone has committed a crime" or "to doubt or not trust".

6.23 These definitions demonstrate the breadth of the concept of suspicion. It encapsulates a variety of states of mind which exist on a spectrum from an imagining or inkling to thinking or perhaps believing something to be true or probable. It is clear from these dictionary definitions that defining suspicion in the POCA context is not going to be straightforward.

---

20 *R v Da Silva* [1996] 2 Cr. App. R. 35.

21 (1972) 56 Cr. App. R. 799 at 804.

22 *Millington and Sutherland Williams on the Proceeds of Crime* (2018), para 20.49.

23 https://chambers.co.uk/search/?query=suspicion&title=21st (last accessed 17 July 2018).

24 https://dictionary.cambridge.org/dictionary/english/suspect (last accessed on 12 May 2018).

Suspicion in the hierarchy of fault

6.24 In this section we consider, in brief, the range of related definitions of fault and where suspicion is placed in this hierarchy to understand the implications of using suspicion as a threshold.

6.25 As academics have recognised, a variety of terms are used in statute to describe states of mind as to elements of the offence. Difficulty arises when attempting to identify the precise parameters of each:

> Knowledge is not the only legislative term to describe prohibited states of mind as to circumstances. Parliament has deployed a range of terms: 'knowledge', 'belief', 'suspicion', 'having reasonable grounds to suspect', and even 'recklessness'. Parliament's use of these different terms clearly supports the view that they do not share the same meaning in law. The argument that these are not synonymous is strengthened considerably by the fact that the terms are used in many offences as alternative *mens rea* requirements. Parliament's use of alternatives alongside knowledge may also indicate recognition of the difficulty that proof of knowledge poses. Judicial interpretation of the different terms in a variety of different offences also makes clear that they are quite distinct. The difficult issue lies in identifying the respective boundaries of each concept.[25]

6.26 In order to understand the boundaries of suspicion and where it falls within the hierarchy of states of mind, we will consider in turn:

(1) knowledge;

(2) "blind-eye" knowledge;

(3) belief;

(4) reasonable grounds/cause to believe;

(5) reasonable grounds/cause for suspicion; and

(6) suspicion.

Knowledge

6.27 Ashworth summarises the position as follows:

> … where the term 'knowingly' appears in an offence or where knowledge is otherwise required, it requires subjective awareness by D of each of the facts and circumstances in the definition of the crime to which it applies.[26]

---

[25] David Ormerod, Making sense of mens rea in statutory conspiracies, Current Legal Problems (2006) p 207.

[26] Andrew Ashworth, *Principles of criminal law* (6th Ed 2009), p 184. We rely on this edition because later editions of this text do not deal with the specific topic of knowledge.

6.28 In addition, Shute observes that knowledge also requires that what is known is also true:

> …all offences which incorporate 'knowledge' of a specified proposition as a necessary element for their commission appear to require that the 'known' proposition be true…[27]

6.29 Whilst knowledge is not the requisite state of mind for the principal money laundering offences, the position is different in respect of a conspiracy to commit an offence under sections 327to 329 of the Proceeds of Crime Act 2002. In *R v Saik*[28] the House of Lords examined the concept of knowledge in the context of section 1 of the Criminal Law Act 1977:

> In this context the word 'know' should be interpreted strictly and not watered down. In this context knowledge means true belief. Whether it covers wilful blindness is not an issue arising on this appeal. As applied to section 93C(2) [the forerunner to POCA] it means that, in the case of identified property, a conspirator must be aware the property was in fact the proceeds of crime. The prosecution must prove the conspirator knew the property was the proceeds of criminal conduct."

6.30 On the distinction between knowledge and suspicion, the Court observed that:

> Suspicion, as a state of mind, is not properly to be analysed and dissected as counsel sought to do. In ordinary usage, and time and again in statutes, a distinction is drawn between suspicion and knowledge. The former is not to be equated with the latter. Section 1(2) explicitly requires a conspirator to 'intend or know' that the relevant fact 'shall or will' exist. That is not the state of mind of a conspirator who agrees to launder money he only suspects may be criminal proceeds. He does not 'intend' the money will be the proceeds of crime, conditionally or otherwise. He simply suspects this may be so, and goes ahead regardless. A decision to deal with money suspected to be the proceeds of crime is not the same as a conscious decision to deal with the proceeds of crime.[29]

"Blind-eye" knowledge or wilful blindness

6.31 In *Roper v Taylor's Central Garages (Exeter) Ltd*[30], Devlin J identified three types of knowledge in a criminal case; actual knowledge (first degree), wilful blindness (second degree) and constructive knowledge (third degree):

> There are, I think, three degrees of knowledge which it may be relevant to consider in cases of this sort. The first is actual knowledge, and that the justices may infer from the nature of the act that was done, for no man can prove the state of another man's mind, and they may find it, of course, even if the defendant gives evidence to the contrary. They may say: 'We do not believe him. We think that was his state of mind.'

---

27 Stephen Shute, Knowledge and Belief in the Criminal Law in Shute, S and Simester, A P, *Criminal Law Theory Doctrines of the General Part* (2001), p 191.

28 [2006] UKHL 18; [2007] 1 A C 18.

29 [2006] UKHL 18; [2007] 1 A C 18 at para 32.

30 [1951] 2 T L R 284

> They may feel that the evidence falls short of that, and, if they do, they have then to consider what might be described as knowledge of the second degree.
>
> They have then to consider whether what the defendant was doing was, as it has been called, shutting his eyes to an obvious means of knowledge. Various expressions have been used to describe that state of mind. I do not think it is necessary to describe it further, certainly not in cases of this type, than by the phrase that was used by Lord Hewart CJ, in a case under this section, *Evans v Dell*[31]. What the Lord Chief Justice said was: 'The respondent deliberately refrained from making inquiries, the results of which he might not care to have.'
>
> The third sort of knowledge is what is generally known in law as constructive knowledge. It is what is encompassed by the words 'ought to have known' in the phrase 'knew or ought to have known.' It does not mean actual knowledge at all, it means that the defendant had in effect the means of knowledge. When, therefore, the case of the prosecution is that the defendant failed to make what they think were reasonable inquiries it is, I think, incumbent on the prosecutor to make it quite plain what they are alleging. There is a vast distinction between a state of mind which consists of deliberately refraining from making inquiries, the result of which the person does not care to have, and a state of mind which is merely neglecting to make such inquiries as a reasonable and prudent person would make. If that distinction is kept well in mind, I think justices will have less difficulty in determining what is the true position. The case of shutting the eyes is actual knowledge in the eyes of the law; the case of merely neglecting to make inquiries is not actual knowledge at all, but comes within the legal conception of constructive knowledge, which is not a conception which, generally speaking, has any place in the criminal law.[32]

6.32 For wilful blindness to apply, an individual may deliberately avoid further inquiry so as not to confirm their suspicion. Suspicion is used as a proxy for knowledge in these circumstances. In a civil context, wilful blindness has been said to require a "clear suspicion"[33] that is "firmly grounded and targeted on specific facts"[34]. In *Manifest Shipping Co Ltd v Uni-Polaris Insurance Co Ltd*, Lord Scott of Foscote said:

> In summary, blind-eye knowledge requires, in my opinion, a suspicion that the relevant facts do exist and a deliberate decision to avoid confirming that they exist. But a warning should be sounded. Suspicion is a word that can be used to describe a state of mind that may, at one extreme, be no more than a vague feeling of unease and, at the other extreme, reflect a firm belief in the existence of the relevant facts. In my opinion, in order for there to be blind-eye knowledge, the suspicion must be firmly grounded and targeted on specific facts. The deliberate decision must be a decision to avoid obtaining confirmation of facts in whose existence the individual has good reason to believe. To allow blind-eye knowledge to be constituted by a decision not to

---

31 [1937] 1 All E R 349.

32 [1951] 2 T L R 284, p 449.

33 *Group Seven Ltd v Nasir* [2017] EWHC 2466 (Ch); [2018] P N L R 6, at 445 and *Att-Gen. of Zambia v Meer Care & Desai (A Firm)* [2008] EWCA Civ 1007; [2008] Lloyd's Rep F C 587.

34 *Manifest Shipping Co Ltd v Uni-Polaris Insurance Co Ltd* [2003] 1 AC 469.

enquire into an untargeted or speculative suspicion would be to allow negligence, albeit gross, to be the basis of a finding of privity.

6.33 In *Barlow Clowes International Ltd v Eurotrust International Ltd*[35], Lord Hoffmann thought that it was "substantially accurate" to say that the judge could not have held [Mr X] liable unless she could find that [X] "had solid grounds for suspicion which he consciously ignored that the disposal in which [he] participated involved dealings with misappropriated trust funds." Requiring a suspicion to be of sufficient strength or on cogent grounds may bridge the divide between a low-level suspicion and a prima facie case.

Reasonable cause to believe/reasonable grounds to believe

6.34 In *Liversidge v Anderson*[36] the House of Lords considered the meaning of "reasonable cause to believe" in the context of the Secretary of State's power to make an order directing that a person be detained pursuant to regulation 18B of the Defence (General) Regulations 1939. The question to be decided was whether the words required that there must be an external fact as to reasonable cause for the belief, and one, therefore, capable of being challenged in a court of law, or whether, as the respondents contend, the words, in the context in which they are found, point simply to the belief of the Secretary of State founded on his view of there being reasonable cause for the belief which he entertains. It was held that a court of law cannot inquire whether in fact the Secretary of State had reasonable grounds for his belief. Dissenting, Lord Atkin stated:

> "Reasonable cause" for an action or a belief is just as much a positive fact capable of determination by a third party as is a broken ankle or a legal right. If its meaning is the subject of dispute as to legal rights, then ordinarily the reasonableness of the cause, and even the existence of any cause is in our law to be determined by the judge and not by the tribunal of fact if the functions deciding law and fact are divided. Thus having established, as I hope, that the plain and natural meaning of the words "has reasonable cause" imports the existence of a fact or state of facts and not the mere belief by the person challenged that the fact or state of facts existed, I proceed to show that this meaning of the words has been accepted in innumerable legal decisions for many generations, that "reasonable cause" for a belief when the subject of legal dispute has been always treated as an objective fact to be proved by one or other party and to be determined by the appropriate tribunal.[37]

6.35 In an investigative context, requiring reasonable grounds does require a court to be satisfied that there was an objective foundation for the belief. For example, POCA empowers a judge to make a restraint order where there is reasonable cause to believe that the alleged offender has benefited from his criminal conduct.[38] In *Windsor and Others v CPS*, Hooper LJ stated:

> Before charge — and all the more so before arrest — there will be many uncertainties. The law does not require certainty at this stage but uncertainty is not in itself a reason

---

35 [2005] UKPC 37, [2006] 1 WLR 1476 at para 19.

36 [1942] AC 206.

37 [1942] AC 206, at 228.

38 Proceeds of Crime Act, s 40(2)(b).

> for making a restraint order as some of the respondent's submissions might suggest. The court must sharply focus on the statutory test: is the judge satisfied that there is a reasonable cause to believe that the alleged offender has benefited from his criminal conduct? It is that test which the court must apply and it requires a detailed examination of the material put before it. The presence of uncertainties does not prevent there being reasonable cause to believe, but the judge must still be satisfied that there is reasonable cause to believe.[39]

Belief

6.36 In *R v Moys*[40] the Court of Appeal considered the definition of belief and its relationship with knowledge and suspicion in the context of handling stolen goods under section 22(1) of the Theft Act 1968. The Court stated that:

> The question is a subjective one and it must be proved that the defendant was aware of the theft or that he believed the goods to be stolen. Suspicion that they were stolen, even coupled with the fact that he shut his eyes to the circumstances, is not enough, although those matters may be taken into account by a jury when deciding whether or not the necessary knowledge or belief existed.

6.37 In *R v Forsyth*[41], a case concerning, in part, the correctness of the trial judge's direction on knowledge or belief, Beldam LJ stated that "even great suspicion was not to be equated with belief." The court observed that "between suspicion and actual belief there may be a range of awareness". Rather, the ordinary meaning of belief was the mental acceptance of a fact as true or existing".[42] Belief is a lesser state of mind than knowledge but requires acceptance of relevant facts. This places it above suspicion in the hierarchy.

6.38 "Reasonable grounds for suspicion" has been described as "a gradation of knowledge".[43] In *R v Saik,*[44] the House of Lords observed that:

> The margin between knowledge and suspicion is perhaps not all that great where the person has reasonable grounds for his suspicion…

6.39 The House held that "reasonable grounds to suspect" required a subjective suspicion supported by objective grounds.[45] This additional requirement of a reasonable basis for the suspicion means that to prove "reasonable grounds to suspect" imposes a greater obligation on the Crown than mere suspicion. However, the term may prescribe a purely objective test depending on the context in which it is used in accordance with the recent

---

39 [2011] EWCA Crim 143 at para 53, [2011] 1 WLR 1519.

40 (1984) 79 Cr App R 72.

41 [1997] 2 Cr App R 299 at p 320.

42 [1997] 2 Cr App R 299 at p 320.

43 *R v Singh* [2003] EWCA Crim 3712 per Auld LJ at para 34.

44 [2006] UKHL 18; [2007] 1 AC 18 at para 30.

45 [2006] UKHL 18; [2007] 1 AC 18 at paras 52-53.

judgment in *R v Sally Lane and John Letts* which is considered below.[46] We will return to examine the concept of reasonable grounds to suspect and its relationship with suspicion in detail later in this Chapter.

Suspicion

6.40 The "ordinary meaning" of "suspicion" was defined by Lord Devlin in *Hussien v Chong Fook Kam*[47] in the exercise of police powers to arrest a suspect:

> ….a state of conjecture or surmise where proof is lacking: 'I suspect but I cannot prove.'

6.41 As we discussed in Chapter 2, the leading case on suspicion in the POCA context is *R v Da Silva*.[48] The Court re-iterated that a trial judge could not be criticised if he or she did not define suspicion for the jury other than to say it was an ordinary English word and the jury should apply their own understanding of it. A judge was not precluded from offering more assistance to the jury. If the judge chose to do so, what was required in the context of the money laundering offences (in the Criminal Justice Act 1988 which preceded the POCA regime) was that:

> the defendant must think that there was a possibility, which was more than fanciful, that the relevant fact existed.

Reasonable cause to suspect

6.42 In the case of *R v Sally Lane and John Letts*[49], the Supreme Court considered the meaning of "reasonable cause to suspect" in the context of section 17b of the Terrorism Act 2000. A person commits an offence under section 17 of the Terrorism Act 2000 if:

(1) he or she enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another, and

(2) he or she knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

6.43 The issue to be decided was whether the expression "reasonable grounds to suspect" in section 17b meant that the accused must actually suspect. Lord Hughes summarised the issue as follows:

> The question which arises on this appeal concerns the correct meaning of the expression "has reasonable grounds to suspect" in section 17(b). Does it mean that the accused must actually suspect, and for reasonable cause, that the money may be used for the purposes of terrorism? Or is it sufficient that on the information known to

---

46 [2018] UKSC 36.

47 [1970] AC 942; [1970] 2 WLR 441.

48 [2006] EWCA 1654, [2006] 2 Cr App R 35.

49 [2018] UKSC 36.

him that exists, assessed objectively, reasonable cause to suspect that that may be the use to which it is put?[50]

6.44 The Court found no difference between the words "grounds" and "cause" for the purposes of the appeal and held that it was not possible to read *Saik*[51] as laying down a universal proposition that if a statute uses the term "reasonable cause to suspect", that will always assume that a person has to have actual suspicion.[52]

6.45 The Court distinguished the language used in the statute from alternative terms such as "knows or suspects" and "knows or reasonably suspects" which denoted subjective suspicion. Lord Hughes observed in relation to section 17b that:

> It does not say what one would expect it to say if it meant that the defendant must be proved actually to have suspected, that is:
>
> "If he knows or suspects…"
>
> Nor for that matter, does it say:
>
> "If he knows or reasonably suspects…"

6.46 This requirement that there exists objectively assessed cause for suspicion would be satisfied when, on the information available to the accused, a reasonable person would suspect that the money might be used for terrorism. For this reason, "reasonable cause to suspect" (or "reasonable grounds to suspect") may set a lower threshold than suspicion where it is construed as a purely objective test. Where it is interpreted as a cumulative test, it may set a higher threshold than mere suspicion.

Suspicion based tests in the investigative context

6.47 In addition to the use of this range of concepts as elements in criminal offences, Parliament has used various forms of suspicion based test in defining investigative powers in a criminal justice context. Many cases involve the exercise of police powers.

Reasonable grounds to suspect/reasonable cause to suspect

6.48 This is a common phrase in criminal law in relation to the exercise of police powers. For example, it is a pre-condition for the power of a police constable to arrest without a warrant in specific circumstances.[53] This approach to suspicion is evident throughout the powers provided for in the Police and Criminal Evidence Act 1984. For example, the power to stop and search an individual for stolen or prohibited articles under section 1 of the Police and Criminal Evidence Act 1984 requires the existence of reasonable

---

50 [2018] UKSC 36, para 4.

51 [[2006] 2 WLR 993, [2006] 2 WLR 993.

52 [2018] UKSC 36, para 17.

53 Police and Criminal Evidence Act 1984, s 24.

grounds for suspicion. PACE Code A gives guidance as to factors which may or may not support reasonable grounds for suspicion.[54]

6.49 The threshold of suspicion means that a police officer can take into account matters which might not necessarily be admissible as evidence in a criminal trial. However, there must be some reasonable, objective grounds for the suspicion, based on known facts and information which are relevant to the likelihood the offence has been committed and the person liable to arrest committed it. Guidance is given on examples of facts and information which might point to a person's innocence and may tend to dispel suspicion.[55]

6.50 In the context of a police investigation, this test is appropriate as the threshold for exercising intrusive powers must balance the suspect's rights to liberty and privacy with the need to advance an investigation. Requiring a prima facie case against a suspect would limit the police's ability to investigate and obtain evidence. In *Hussien v Chong Fook Kam*[56], Lord Devlin stated:

> Suspicion arises at or near the starting-point of an investigation of which the obtaining of prima facie proof is the end.[57]

6.51 Where reasonable grounds are required for a suspicion in an investigative context, the courts' general approach has been to interpret this as a cumulative test requiring both a subjective and an objective element. The additional requirement of reasonableness operates as a safeguard against subjective hunches or instinct. In *O'Hara v Chief Constable of the Royal Ulster Constabulary*[58] the Court considered the meaning of "reasonable grounds for suspecting" in the context of section 12 of the Prevention of Terrorism (Temporary Provisions) Act 1984. The House of Lords held that the test was partly subjective and partly objective; the arresting officer must have formed a genuine suspicion that the person being arrested had been concerned in acts of terrorism, and there had to be reasonable grounds for forming such a suspicion. This meant that a reasonable person would have also reached the same conclusion based upon the information available.

6.52 In *O'Hara v UK*[59], the applicant's case was considered before the European Court of Human Rights. The ECHR considered the issue of "reasonable suspicion" in determining whether the applicant's arrest and subsequent detention had violated Article 5 of the European Convention on Human Rights. The Court held that it was an essential component of the safeguard contained in Article 5.1(c) of the Convention that

---

54 See for example Police and Criminal Evidence Act 1984 Code A, Revised Code of Practice for the exercise by: police officers of statutory powers of stop and search, police officers and police staff of requirements to record public encounters, paras 2.1 to 2.2.

55 Police and Criminal Evidence Act 1984 s 24(2) (as substituted: see note 4) and Code G para 2.3A and Note 2A. See for example *Parker v Chief Constable of Essex* [2017] EWHC 2140 (QB).

56 [1970] AC 942; [1970] 2 WLR 441.

57 [1970] AC 942 at 948(B).

58 [1997] A C 286; [1997] 2 WLR1. See also *Fitzpatrick and others v The Commissioner of Police of the Metropolis* [2012] EWHC 12 (QB).

59 *O'Hara v United Kingdom* (2000) app no. 37555/97.

any suspicion on which an arrest was based should be reasonable and, therefore, based upon objective grounds capable of providing justification to a third party. This requires the existence of some facts or information which would satisfy an objective observer that the person concerned may have committed the offence, though what may be regarded as reasonable will depend on all the circumstances of the case.

6.53 "Reasonable cause to suspect" is another suspicion-based test deployed within the investigative context. The meaning of "reasonable cause to suspect" was considered in *A-G of Jamaica v Williams.*[60] The Privy Council considered the power of a court to grant a warrant under section 203 of the Customs Act holding that it must appear to the court, from information on oath, "that the officer has reasonable cause to suspect one or more of the matters there specified":

> It is not sufficient that the justice is satisfied by the officer's oath that he suspects; it must appear to the justice that his cause for suspicion is reasonable. The test is an objective one.

6.54 In *McAughey v HM Advocate*[61] Scotland's High Court of Justiciary held that the test for reasonable grounds for suspicion in section 23 of the Misuse of Drugs Act 1971 "relates to what is in the mind of the arresting officer when the power is exercised". An individual must form their own suspicion and cannot rely solely on what they have been told:

> The test is in part subjective, in that the arresting officer must have formed a genuine suspicion in his own mind that the person is in possession of a controlled drug. The fact that someone else, however eminent or worthy of credit, has such a suspicion, is not good enough.

6.55 In *Parker v The Chief Constable of Essex Police* (High Court),[62] Stuart-Smith J observed that assessing the quality and reliability of information was an essential part of the process:

> Whatever the nature of the material that is said to provide the basis for the reasonable suspicion, the weight that may reasonably be attached to it will depend upon its quality and apparent reliability. Assessment of the quality and reliability of the material is an essential part of any reasonable process of arriving at a basis for suspicion.

6.56 These cases must be read in light of the judgment in *R v Sally Lane and John Letts*[63] in which the Court stated that *Saik*[64] and *O'Hara*[65] could not be read as laying down a universal proposition that "reasonable cause to suspect" would always require actual

---

60 [1998] A C 351.

61 [2013] HCJAC 163.

62 [2017] EWHC 2140 (QB).

63 [2018] UKSC 36.

64 [22006] UKHL 18, [2006] 2 WLR 993.

65 [1997] AC 286; [1997] 2 WLR 1.

suspicion. The meaning of the term will be dependent upon the context in which it is used. In section 17b of the Terrorism Act 2000, it was a wholly objective test.

6.57 Considerations of strength and standards of suspicion frequently arise in the context of decisions on powers exercisable by law enforcement agencies. As Penney observes:

> Perhaps the most important way that the law regulates police and other law enforcement agents is by articulating standards of suspicion, i.e., the nature and degree of justification needed to intrude into legally protected realms of liberty and privacy.[66]

6.58 The advantage of a cumulative test which marries suspicion with reasonable grounds or cause is that it benefits law enforcement agencies whilst providing an additional layer of protection for suspects against intrusion by the authorities.

US law on suspicion in an investigative context

6.59 The phrase "articulable cause" has been used in US jurisprudence on the issue of pre-arrest detention for investigative purposes.[67] The issue of "articulable cause" has arisen where there is no reasonable and probable cause to arrest a suspect but there is some suspicion of criminal activity triggering a need to investigate. Articulable cause suggests a subjective suspicion with some verifiable facts at its foundation and may therefore fall below "reasonable grounds to suspect". In *Terry v Ohio* the idea of "articulable cause" was expressed by Chief Justice Warren in these terms:

> …in justifying the particular intrusion, the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion…[68]

6.60 In *US v Cortez*[69], the Supreme Court observed that qualitative phrases such as "articulable reasons" or "founded suspicion" were not self-defining and fell short of providing clear guidelines. As Young argues, establishing abstract standards of evaluation does not assist the officer on the street in determining when it is legitimate to act. The same argument may apply to reporters who are applying *Da Silva*[70].

Canadian law on suspicion in an investigative context

6.61 In *R v Simpson*[71], the Court considered whether a police officer was permitted to detain an individual at common law for investigative purposes where the grounds for an arrest where not met. The Court referred to the need for some articulable cause for the detention based on "a constellation of objectively discernible facts". A hunch based entirely on intuition gained by experience would not be sufficient. Importantly, the Court

---

66 S Penney, Standards of Suspicion, Criminal Law Quarterly December 2017, p 23.

67 See for example *R v Simpson* 12 OR (3d) 182; [1993] OJ No 308, *Terry v Ohio* 392 US 1, 88 S; Ct 1868 (1968).

68 392 US 1 88 S at p 21.

69 449 US 411 (1981) at 417 to 418.

70 [2006] EWCA Crim 1654, [2007] 1 WLR 303 and see Alan Young, All Along the Watchtower: Arbitrary Detention and the Police Function, 29 Osgoode Hall Law Journal 329 (1991) at 378.

71 12 OR (3d) 182; [1993] OJ No 308.

noted that objective criteria acted as a safeguard against an officer relying on irrelevant and potentially discriminatory factors:

> Such subjectively based assessments can too easily mask discriminatory conduct based on such irrelevant factors as the detainee's sex, colour, age, ethnic origin or sexual orientation. Equally without objective criteria detentions could be based on mere speculation. A guess which proves accurate becomes in hindsight a "hunch".

6.62 Young notes that it has been recognised that not all factors must be left to the "subjective weighting of the officer." Common factors, shown to have "predictive capabilities" can provide guidance to those making decisions on suspicion:

> A stated policy mandates a presumptive weighting of certain factors that have been shown to have predictive capabilities.

6.63 Whilst a list could never be exhaustive, common factors or indicators could be considered and included in guidance to encourage decisions on suspicion to be evidence-based rather than instinctive or "subjective hunches". This is precisely what has been achieved in an investigative context within the Codes of Practice issued pursuant to the Police and Criminal Evidence Act 1984. However, this is not an approach utilised in relation to Part 7 of the Proceeds of Crime Act 2002.

6.64 We will now consider the various suspicion based tests that are found in the Proceeds of Crime Act 2002.

Suspicion-based tests in the Proceeds of Crime Act 2002

6.65 The Proceeds of Crime Act 2002 refers to various suspicion-based tests: "knows or suspects"[72], "know or suspect"[73]; "suspecting"[74]; "suspect"[75] and "suspects".[76]

6.66 Other provisions of that Act refer to an additional requirement of reasonableness such as "reasonable grounds to suspect"[77], "has reasonable grounds for suspecting"[78], "reasonable grounds for knowing or … suspecting"[79], or "continuing grounds to suspect".[80]

6.67 The Proceeds of Crime Act 2002 does not define any of these suspicion-based tests. Our focus in the next Chapter will be on the application of suspicion specifically in

---

72 Proceeds of Crime Act 2002, ss 330(2)(a), 331(2)(a), 332(2) and 338(2A)(c).

73 Proceeds of Crime Act 2002, ss 337(3)(a), 338(2A)(b),

74 Proceeds of Crime Act 2002, s338.

75 Proceeds of Crime Act 2002, s 340(3).

76 Proceeds of Crime Act 2002, ss 328(1) and 330(2)(a).

77 e.g. Proceeds of Crime Act 2002, ss 40, 317, 321, 322 and 471.

78 Proceeds of Crime Act 2002, s 127C.

79 Proceeds of Crime Act 2002, ss 330(2)(b) and 337(3)(b).

80 Proceeds of Crime Act 2002, s 339ZD(5).

relation to the money laundering offences under sections 327, 328 and 329 of the Proceeds of Crime Act 2002.

COMMISSION OF INQUIRY INTO STATE CAPTURE

Chapter 7: The application of the concept of suspicion in the context of the money laundering offences

7.1 The principal money laundering offences under the Proceeds of Crime Act 2002 ("POCA") regime require proof only that the property was or represented the proceeds of crime and that the accused had a suspicion that the property constituted such proceeds.[1] As we observed in the previous Chapter, this is an unusually low threshold for a criminal offence.

7.2 There is a second aspect to these offences which we must also consider. Where an individual in the reporting sector suspects that they are dealing with criminal property, this will trigger an authorised disclosure to protect against criminal liability for the sections 327 to 329 offences.[2]

7.3 Such reporting provides opportunities for investigators to identify suspected criminal property when dealings with it are being contemplated or even carried out, allowing intervention at a crucial stage in the process of money laundering. Setting the threshold for criminal liability at the threshold of suspicion means that the trigger for the reporting is a light one and therefore, law enforcement agencies are the principal beneficiaries. This inter-relationship between the money laundering offences and the ability to generate intelligence is an important feature of the anti-money laundering regime.

7.4 In the following section, we will examine how the courts have interpreted the concept of suspicion in the context of money laundering offences.

CASE LAW ON SUSPICION IN THE CONTEXT OF MONEY LAUNDERING OFFENCES

7.5 As we discussed in Chapter 2, the interpretation of suspicion in *R v Da Silva* has been adopted by the courts and is used as a guiding principle by those in the reporting sector.[3] In *Da Silva*, the Court of Appeal considered the correct interpretation of suspicion within the meaning of section 93A(1)(a) of the Criminal Justice Act 1988.[4] It was interpreted to mean:

> … a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to

---

1 This is, of course, subject to the individual performing one of the specific acts prohibited under the Proceeds of Crime Act 2002, ss 327, 328 and 329.

2 Proceeds of Crime Act, ss 327 to 329.

3 [2006] EWCA Crim 1654, [2007] 1 W L R 303.

4 This Act preceded the Proceeds of Crime Act 2002.

be 'clear 'or 'firmly grounded and targeted on specific facts', or based upon 'reasonable grounds'.[5]

7.6 The Court went on to consider whether it was necessary for the person's suspicion to be of a more settled nature. A defendant might entertain a suspicion but, on further thought, dismiss it from his or her mind as being unworthy, contrary to such evidence as existed or outweighed by other considerations. The Court left this open as a possible direction to the jury in an appropriate case on the facts.[6]

7.7 Referring to POCA[7], the Court observed that the statute deliberately distinguished between the word 'suspicion' and at other times, 'reasonable grounds for suspicion'. A requirement to prove reasonable grounds could not simply be inferred where the statute referred solely to suspicion.[8] The Court declined to imply the word 'reasonable' into the statutory provision.

7.8 *Da Silva*[9] was applied in the Civil Division of the Court of Appeal in *K v National Westminster Bank*.[10] It has also been applied in a number of other cases on Part 7 of the Proceeds of Crime Act 2002.[11]

7.9 The Court in *Da Silva* did not articulate a standard of suspicion based on strength or degree, for example by requiring there to be objective grounds for it or requiring it to be reasonable. Indeed, there is no reasonableness requirement in section 340 of the Proceeds of Crime Act 2002. However, as some commentators have observed the Court's rejection of "inkling" taken from the ordinary dictionary definition of suspicion indicated that a suspicion should have some basis:

> The court is right, it is submitted, not formally to impose a gloss on the definition as it applies in this statutory offence by requiring that the suspicion be "clear" or "firmly grounded and targeted on specific facts", even though that approach has been adopted by the House of Lords in various civil law contexts. However, the court's rejection of the use of "inkling", etc. suggests that juries ought to be encouraged to look for some foundation for the defendant's alleged suspicion.[12]

---

5 [2007] 1 WLR 303; [2006] EWCA Crim 1654 at [16].

6 [2007] 1 WLR 303; [2006] EWCA Crim 1654 at [17].

7 Proceeds of Crime Act 2002.

8 [2007] 1 WLR 303; [2006] EWCA Crim 1654 at [9 to 10]. See also *R v Saik* [2006] UKHL 18 and *Ahmad v HM Advocate* [2009] HCJAC 60; [2009] SCL1093.

9 [2006] EWCA Crim 1654, [2007] 1 W L R 303.

10 [2007] 1 WLR 311, [2006] EWCA Civ 1039.

11 *Parvizi v Barclays Bank* [2014] EWHC B2 (QB), *Shah v HSBC* [2010] EWCA Civ 31, [2010], *Sitek v Circuit Court in Swidnica, Poland* [2011] EWHC 1378 (Admin).

12 David Ormerod, Proceeds of crime: assisting another to retain benefit of criminal conduct knowing or suspecting other person to be engaged in criminal conduct, (2007) *Criminal Law Review*, Jan, p 79.

Reasonable grounds for suspicion in the context of money laundering offences

7.10 We can now turn to consider the application of the alternative fault threshold which applies in Part 7.

7.11 Prior to the enactment of the principal money laundering offences in Part 7 of the Proceeds of Crime Act 2002, "reasonable grounds to suspect" was used to describe the threshold for a money laundering offence in section 93C(2) of the Criminal Justice Act 1993. In *R v Saik,*[13] the House of Lords considered the wording of section 93C(2) of the Criminal Justice Act 1993,[14] "knowing or having reasonable grounds to suspect that any property is the proceeds of criminal conduct".

7.12 There were two possible interpretations considered. A mixed test would combine a subjective element (that the offender actually suspected) and an objective element (that the suspicion was based on reasonable grounds). The alternative interpretation was that the fault element of "reasonable grounds to suspect" was purely objective. On the latter interpretation, it would require proof only that a reasonable person ought to have suspected the criminal nature of the property based on the information available.[15] Lord Hope analysed the wording and stated:

> "Section 93C(2) requires proof of what the defendant knew or had reasonable grounds to suspect on the one hand, and of the purpose for which he engaged in the activities that the subsection prescribes on the other. The appellant submits that there is an incompatibility between these two requirements…
>
> I think the apparent mismatch between these two requirements is based on a misunderstanding of what the first proposition involves. The test as to whether a person has reasonable grounds to suspect is familiar in other contexts, such as where a power of arrest or of search is given by statute to a police officer. In those contexts, the assumption is that the person has a suspicion, otherwise he would not be thinking of doing what the statute contemplates. The objective test is introduced in the interests of fairness, to ensure that the suspicion has a reasonable basis for it. The subjective test — actual suspicion — is not enough. The objective test, that there were reasonable grounds for it, must be satisfied too. In *O'Hara v Chief Constable of the Royal Ulster Constabulary [1997] AC 286,* where the issue related to the test in section 12(1) of the Prevention of Terrorism (Temporary Provisions) Act 1984 which gave power to a constable to arrest a person without warrant if he had reasonable grounds for suspecting that he was concerned in acts of terrorism, I said at p 298A–C:
>
>> "In part it is a subjective test, because he must have formed a genuine suspicion in his own mind that the person has been concerned in acts of terrorism. In part also it is an objective one, because there must also be reasonable grounds for the suspicion which he has formed. But the application of the objective test does not require the court to look beyond what was in the mind of the arresting officer. It is the grounds which were in his mind at the time

---

13 [2006] UKHL 18, [2006] 2 WLR 993.

14 This Act preceded the Proceeds of Crime Act 2002 and is now repealed.

15 *Smith, Hogan, and Ormerod's Criminal Law* (2018), para 3.2.8.2.

> which must be found to be reasonable grounds for the suspicion which he has formed."

The words used in section 93C(2) can, in my opinion, be analysed in the same way. By requiring proof of knowledge or of reasonable grounds to suspect that the property was criminal proceeds, the subsection directs attention in the case of each of these two alternatives to what was in the mind of the defendant when he engaged in the prohibited activity. Proof that he had reasonable grounds to suspect the origin of the property is treated in the same way as proof of knowledge. The subsection assumes that a person who is proved to have had reasonable grounds to suspect that the property had a criminal origin did in fact suspect that this was so when he proceeded to deal with it. A person who has reasonable grounds to suspect is on notice that he is at the same risk of being prosecuted under the subsection as someone who knows. It is not necessary to prove actual knowledge, which is a subjective requirement. The prosecutor can rely instead on suspicion. But if this alternative is adopted, proof of suspicion is not enough. It must be proved that there were reasonable grounds for the suspicion. In other words, the first requirement contains both a subjective part — that the person suspects — and an objective part— that there are reasonable grounds for the suspicion."[16]

7.13 Baroness Hale also observed that:

> In common with all of your Lordships, I agree that the substantive offence requires that the accused actually suspects that the money is the proceeds of crime.[17]

7.14 The *Saik*[18] interpretation of "reasonable grounds to suspect" has been widely understood as a cumulative test. In *R v Suchedina*, the substantive offences under consideration were section 49(2) of the Drug Trafficking Act 1988 and section 93C(2) of the Criminal Justice Act 1988 (the latter provision having been directly considered in *Saik*[19]), Hughes LJ stated:

> For both of those substantive offences referred to, the mens rea is either knowledge or suspicion of illicit origin. In accordance with the law as it was understood at the time, the trial Judge directed the jury that this offence was made out, as to mens rea, by proof either of knowledge or of reasonable grounds for suspicion that money to be handled was at least in part of illicit origin of one kind or the other. For the reasons explained in *Saik* that was a misdirection in two ways. First, even for the substantive offences, what matters is actual suspicion, rather than objectively seen reasonable grounds for it. More importantly, for conspiracy, only intention or knowledge will suffice, and suspicion will not.[20]

---

16 [2006] UKHL 18; [2007] 1 AC 18 at paras 51 to 53.

17 [2006] UKHL 18; [2007] 1 AC 18 at paras 102.

18 [2006] UKHL 18; [2007] 1 AC 18.

19 [2006] UKHL 18; [2007] 1 AC 18.

20 [2006] EWCA Crim 2543; [2007] 1 Cr App R. 23,

7.15 In *R v Sally Lane and John Letts,* Lord Hughes acknowledged that the cumulative test was one legitimate interpretation of "reasonable grounds to suspect". Referring to section 93C(2) of the Criminal Justice Act 1988, Lord Hughes stated:

> It is certainly true that in *Saik* the House of Lords concluded that this section imported a requirement that the defendant actually suspect, as well as that he did so on reasonable grounds.[21]

7.16 The principal benefit of a cumulative test requiring both a subjective and an objective limb is that it provides an additional safeguard for an accused person. Following a *Saik*[22] approach, a person avoids criminal liability where he or she merely ought to have suspected that property was criminal property, given the grounds that existed at the time, but did not personally suspect that fact. The *Saik*[23] interpretation requires a defendant to be proved to have actually suspected that the property was criminal in order to be convicted.[24]

7.17 In the next section, we will examine the various sources of non-statutory guidance available to the reporting sector on how to apply suspicion in practice.

Guidance on suspicion

7.18 There is no consistent interpretation of suspicion across the sector-led guidance documents. Reporters can consult guidance from a number of non-statutory sources. The National Crime Agency ("NCA") defines a Suspicious Activity Report ("SAR") as a piece of information which alerts law enforcement agencies that certain client or customer activity is in some way suspicious and might indicate money laundering or terrorist financing.[25] Bosworth-Davies observes that although it is the duty of financial practitioners to disclose suspicious financial transactions to the relevant authorities, there is a lack of clarity as to what a financial practitioner would find to be suspicious.[26]

7.19 The Joint Money Laundering Steering Group Guidance[27] on suspicious activity reporting describes a core obligation on staff to raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge

---

21 [2018] UKSC 36, para 16.

22 [2006] UKHL 18; [2006] 2 WLR 993.

23 [2006] UKHL 18; [2006] 2 WLR 993.

24 It is less clear, in the context of section 330 and 331 of the Proceeds of Crime Act 2002, whether the *Saik* approach applies. Both offences provide four separate ways of committing the offence which includes both "suspicion" and "reasonable grounds to suspect" in contrast to *Saik*. These provisions have yet to be tested in the courts. We will examine these offences later in this Paper.

25 National Crime Agency, *Suspicious Activity Reports Annual Report* (2017) p 6.

26 Rowan Bosworth-Davies, "Money Laundering: chapter five and the implications of global money laundering laws" (2007) 10 *Journal of Money Laundering Control* 189 at 198.

27 The Joint Money Laundering Steering Group (JMLSG) is made up of UK Trade Associations in the Financial Services Industry. It cites its aims as promulgating good practice and giving practical assistance in interpreting the UK Money Laundering Regulations. See http://www.jmlsg.org.uk/what-is-jmlsg.Joint Money Laundering Steering Group Prevention of money laundering/combating terrorist financing: Guidance for the UK Financial Sector (Part 1) 2017 (approved 5th March 2018) See http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current (last accessed 20 June 2018), chapter 6.

or suspicion, that another person is engaged in money laundering, or that terrorist property exists. The firm's nominated officer must consider each report, and determine whether it gives grounds for knowledge or suspicion.

7.20 Defining suspicion, the guidance states that:

> Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example:
>
> A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not; and
>
> Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation.[28]

7.21 The guidance also offers assistance on the concept of reasonable grounds to suspect[29] and lists factors to consider such as: the nature/origin of the transaction; how the funds; cash or asset(s) were discovered; the amounts or values involved; their intended movement and destination; how the funds cash or asset(s) came into the customer's possession; and whether the customer(s) and/or the owners of the cash or asset(s) (if different) appear to have any links with criminals/criminality, terrorists, terrorist groups or sympathisers, whether in the UK or overseas.

7.22 The Law Society's guidance draws a distinction between cause for concern and suspicion. The guidance suggests that suspicion may arise from something unusual or unexpected and after making enquiries, the facts do not seem normal or make commercial sense.[30]

7.23 Guidance produced by the Consultative Committee of Accountancy Bodies ("CCAB") for the accountancy profession differs in its explanation. It acknowledges that there is very little definitive guidance on what constitutes 'suspicion' so the concept remains subjective. The guidance refers to a state of mind more definite than speculation but falling short of evidence-based knowledge; a positive feeling of actual apprehension or mistrust; a slight opinion, without sufficient evidence.[31]

7.24 Several points are worth noting about the range of guidance that has evolved:

---

28 Joint Money Laundering Steering Group Prevention of money laundering/combating terrorist financing: Guidance for the UK Financial Sector (Part 1) 2017 (approved 5th March 2018) See http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current (last accessed 20 June 2018), paras 6.2 and 6.11.

29 In respect of Proceeds of Crime Act 2002, ss 330 (2)(b) and 331 (2)(b), and Terrorism Act, s 21A.

30 Law Society *Guidance on Anti-Money Laundering* (2017) p 88.

31 CCAB *Anti-Money Laundering – Guidance to the Accountancy Sector* (2018) http://www.ccab.org.uk/documents/TTCCABGuidance2017regsAugdraftforpublication.pdf (last visited 20 June 2018), para [6.1.5].

(1) the large number of documents produced by various parts of the regulated sector suggest a clear demand for guidance;

(2) individual sectors may benefit from guidance which gives examples and assistance specific to the relevant business practices;

(3) it is counter-productive and inefficient to have multiple interpretations of the law across several different documents;

(4) not all of the available guidance is consistent and different sectors may receive contradictory advice on the application of the law;

(5) whilst some of this guidance is approved by HM Treasury, and may be taken into account by a court,[32] ultimately it does not have the force of law;

(6) the burden on those seeking to apply the guidance may outweigh its benefits to them. In 2016, the Joint Treasury and Home Office Action Plan highlighted the issues created by multiple sources of non-statutory guidance. The large number of supervisors resulted in a substantial amount of guidance which was long and challenging to understand. In particular, stakeholders found that there was insufficient clarity around the difference between minimum legal requirements and best practice. Often banks and businesses were forced to familiarise themselves with multiple sources of guidance without specific or practical advice on how to comply with their legal obligations.[33] Since 2016, action has been taken to streamline the approvals process to ensure greater consistency. Guidance documents have been consolidated to provide one guidance document for each sector. However, this still means that there are multiple documents providing guidance on the law and consistency issues still remain.

Criticisms of the suspicion test in the context of money laundering offences

7.25 The application by reporters of the test of suspicion in *Da Silva*[34] has been the subject of criticism. Alldridge noted that:

> This has the effect that if the person in the regulated sector has an inkling that the client has an inkling that the property in question is of dubious provenance, then reports should be made. The consequence is that far more reports are made in the UK than in comparable jurisdictions.[35]

7.26 Marshall has commented that the boundary between unease and suspicion is unrealistic and difficult to identify:

> The problem presented by the test adumbrated by the Court of Appeal is that the boundary between a real but 'vague feeling of unease' and the thought that there is 'a

---

32 Proceeds of Crime Act 2002, ss 330(8) and 331(8).

33 Home Office and HM Treasury *Action plan for anti-money laundering and counter-terrorist finance* (2016), p 50-51.

34 [2006] EWCA Crim 1654, [2006] 2 Cr App R 35.

35 Peter Alldridge, *What went wrong with money laundering law* (2016) p 40.

more than fanciful possibility' that a transaction might constitute a money laundering offence" or that someone is engaged in money laundering, is easy to articulate but in practice likely to be near impossible to identify. The dilemma facing any person considering making a report is the question at what point misgivings become suspicion. Perhaps it is only lawyers who are prone to make such nice linguistic and conceptual distinctions. But a SAR made one side or the other of that, difficult to locate, conceptual boundary may give rise to criminal or civil liability if the one is mistaken for the other.[36]

7.27 In summary, difficulties have been created by the use of the term suspicion as a threshold which triggers duties to report (in the disclosure offences) and effectively imposes duties to make authorised disclosures by those in the sector if they are to avoid liability for the principal money laundering offences. In the absence of further interpretation and guidance from the appellate courts, those burdened with the obligation to report are left without clarity and exposed to criminal liability.

Challenges created by the suspicion test in the context of money laundering offences

7.28 Whilst the test of suspicion has the simplicity of being an ordinary concept, it has no precise boundaries. Different standards and strengths of suspicion may be applied by those making authorised disclosures.

7.29 Our pre-consultation discussions with stakeholders, reveal mixed views towards the interpretation of suspicion adopted in *Da Silva*[37] and the impact that has on the application of the test of suspicion in practice. Three themes emerged:

(1) **Inconsistent application**: stakeholders with reporting obligations were applying different standards of suspicion. This lead to inconsistency between reporters which was apparent during discussions. In addition, standards differed across institutions and sectors. One reporter's mild concern might be another's suspicion. There were differences of opinion as to which factors might indicate suspicion and require a disclosure.

(2) **Poor quality disclosures**: a significant number of SARs were submitted where the grounds for suspicion were not articulated clearly, requiring the NCA to request further information from the reporter. Some disclosures were submitted out of "an abundance of caution" where there was no actual suspicion.[38]

(3) **Confusion as to the law**: stakeholders with reporting obligations found multiple sources of non-statutory guidance confusing. They felt that there should be one set of legal guidance on suspicion.

7.30 The low threshold for criminality creates two issues for those in the reporting sector. First, those in the reporting sector bear an administrative burden from policing this low threshold. Secondly, the individuals incur a risk of liability for an offence carrying a

---

36 Paul Marshall, 'Does Shah v HSBC Private Bank Ltd make the anti-money laundering consent regime unworkable?'' May 2010, *Butterworths Journal of International Banking and Financial Law*, p 287.

37 [2006] EWCA Crim 1654, [2006] 2 Cr. App. R. 35.

38 Interview with UKFIU staff.

maximum of 14 years' imprisonment.[39] As we discussed in Chapter 2, once an authorised disclosure is made, if appropriate consent is granted, the reporter is protected from criminal liability.[40] That protection is not dependent on the test being set as one of suspicion; the same level of protection could be afforded the reporter irrespective of the threshold of fault set for the offence.

7.31 Notwithstanding that there are some reciprocal benefits to law enforcement agencies and reporters from an authorised disclosure exemption, the application of the test of suspicion may create further difficulties in practice. A reporter's subjective suspicion may be irrational, illogical or based on slender evidence. This may weaken the value of any potential disclosure and have a severe and unwarranted financial impact on the subject of a report. As Brown and Evans have highlighted, there is limited scope to challenge a reporter's suspicion:

> In most cases, the statement by those making a SAR that they have a suspicion will be enough. It will be exceptional for the courts to require those that report a suspicion to provide justification for having a suspicion.[41]

7.32 Those who are most disadvantaged by the level being set at mere suspicion are the individuals seeking to make transfers or other dealings with property. The bank customer whose "suspicious" transaction is stopped rendering his or her account frozen can be seriously disadvantaged by such a low threshold trigger.

7.33 Requiring a higher threshold for criminality such as belief or knowledge that property was criminal would benefit the reporting sector (because fewer reports would have to be made) and individuals who are the subject of a disclosure (because it would reduce the risk that legitimate financial transactions are impeded). However, such thresholds might drastically reduce the number of investigative opportunities for law enforcement agencies and limit the prospects to disrupt criminal activity and/or recover criminal assets. This is because a higher threshold for the money laundering offences would have a direct impact on authorised disclosures. As authorised disclosures stop further transactions until a decision is made on appropriate consent (subject to the statutory time limits), they are vital to law enforcement agencies.

7.34 It is next to impossible for those in the regulated sector to avoid committing a criminal offence with such a low threshold if they are to process the millions of transactions customers make. The authorised disclosure exemption can be seen as mitigating this risk of liability.

7.35 The courts have recognised that a balance must be struck. Indeed, in the case of *K Ltd v National Westminster Bank*[42], the Court referred to Part 7 of the Proceeds of Crime Act 2002 as providing "a precise and workable balance of conflicting interests."

---

39 Of course, those who make authorised disclosures in accordance with Part 7 of the Proceeds of Crime Act 2002 are protected from criminal liability.

40 This is subject to Proceeds of Crime Act 2002, ss 327(2), 328(2), 329(2) and 338.

41 G Brown and T Evans, 'The impact: the breadth and depth of the anti-money laundering provisions requiring reporting of suspicion activities', *Journal of International Banking Law Regulations* (2008) 274 to 277 at 275.

42 [2006] EWCA Civ 1039 at [22], [2007] 1 W L R 311.

7.36 The difficulties in balancing the separate interests of law enforcement agencies, reporters, innocent third parties and those who are the subject of a disclosure were highlighted by Laddie J in *Squirrell Ltd v National Westminster Bank:*

> Before analysing the relevant statutory provisions, I should say that I have some sympathy for parties in Squirrell's position. It is not proved or indeed alleged that it or any of its associates has committed any offence. It, like me, has been shown no evidence raising even a prima facie case that it or any of its associates has done anything wrong. For all I know it may be entirely innocent of any wrongdoing. Yet, if POCA has the effect contended for by Natwest and HMCE[43], the former was obliged to close down the account, with possible severe economic damage to Squirrell. Furthermore, it cannot be suggested that either Natwest or HMCE are required to give a cross undertaking in damages. In the result, if Squirrell is entirely innocent it may suffer severe damage for which it will not be compensated. Further, the blocking of its account is said to have deprived it of the resources with which to pay lawyers to fight on its behalf. Whether or not that is so in this case, it could well be so in other, similar cases. Whatever one might feel were Squirrell guilty of wrongdoing, if, as it says, it is innocent of any wrongdoing, this can be viewed as a grave injustice… It is not for the courts to substitute their judgment for that of the legislature as to where the balance should be drawn. If, as [Counsel] says is the case here, the legislation is clear, the courts cannot require a party to contravene it. [44]

7.37 In the next Chapter, we will consider the application of suspicion in the context of the disclosure offences in sections 330 to 332 of POCA. We will then consider the options for reform and how we might balance the separate and competing interests of law enforcement agencies, the reporting sector and those who are the subject of a disclosure to the UKFIU.

---

43 Her Majesty's Customs and Excise.

44 [2005] EWHC 664 (Ch), at [7], [2006] 1 W L R 637.

Chapter 8: The application of the test of suspicion in the context of the disclosure offences

8.1 As discussed in Chapter 2, if a reporter fails to make a required disclosure in accordance with their obligations under Part 7 of the Proceeds of Crime Act 2002 ("POCA"), they may be liable for prosecution for one of the three disclosure offences. Their liability will depend on their status and whether they were acting within or outside the regulated sector.[1]

8.2 Suspicion sets a low threshold for these offences. A reporter who fails to report is committing a crime. This obligation to disclose information in relation to a customer or client backed by criminal sanction is unusual. On the one hand suspicion renders that a very onerous obligation since it requires reporters to be vigilant and report in high volume. On the other hand, the low threshold requires only minimal effort from reporters – there is no need to enquire too closely once suspicion is established.

8.3 In addition, the threshold for reporting in sections 330 and 331 uses a four-part test which we have not examined so far in this Paper. In short, (and subject to other conditions), an individual in the regulated sector has an obligation to make a required disclosure where they know or suspect, or have reasonable grounds for knowing or suspecting that another person is engaged in money laundering.

8.4 In the next section, we will consider how the regulated sector disclosure offences in sections 330 and 331 work in practice. We will use two examples to illustrate the process of making a required disclosure. We have used the example of a bank but a similar process would apply to other businesses and professionals as these offences apply to the regulated sector as a whole. However, internal procedures for monitoring suspicious activity may differ depending on the nature of the business.

The disclosure offences

8.5 The obligation to make a required disclosure (subject to the other conditions and exemptions in sections 330 to 331 of POCA arises where a person in the regulated sector "knows or suspects", or "has reasonable grounds for knowing or suspecting" that another person is engaged in money laundering and does not make a required disclosure as soon as is practicable.[2] Section 332 applies to nominated officers outside of the regulated sector and only requires knowledge or suspicion, not reasonable grounds to know or suspect.

Example 1: Section 330 and the bank cashier

8.6 A cashier serves a customer who has received an unexplained electronic transfer of £5,000 into his account. The customer indicates that he wants to immediately withdraw

---

1 Proceeds of Crime Act 2002, ss 330, 331 and 332.

2 This is intended to provide a brief summary. A full discussion of the disclosure offences can be found in Chapter 2 of this Paper.

the money in £50 notes. He insists the cashier conduct the transactions immediately. The cashier:

(1) Knows or suspects (or has reasonable grounds for knowing or suspecting) that another person is engaged in "money laundering"; without further context, the customer's urgent instructions bear the hallmarks of an unsophisticated attempt to place criminal funds in the financial system and launder them immediately.

(2) Knows the customer's identity, home address and bank details and the whereabouts of the suspected criminal property.

8.7 In the circumstances, if the cashier fails to disclose their suspicion as soon as practicable to the bank's nominated officer[3] (the "required disclosure"[4]) he or she is liable to be prosecuted for a criminal offence.[5] Between 2013 and 2016, 58 cases were prosecuted to trial under section 330 of POCA. A further 1,358 cases resulted in a criminal investigation but did not proceed to a trial.[6]

8.8 As we outlined in Chapter 2, once the cashier submits their internal report, their obligation to disclose has been satisfied.[7] The focus shifts to the nominated officer who has separate obligations to fulfil under section 331 of the Proceeds of Crime Act 2002.

Example 2: Section 331 and the nominated officer

8.9 The nominated officer's obligation to disclose only arises where they receive an internal report from another person (pursuant to section 330 of POCA) informing them of knowledge or suspicion of money laundering. In this example, once the cashier had submitted their internal report to the nominated officer, the nominated officer would need to review the cashier's grounds for suspicion and decide whether or not to submit a suspicious activity report ("SAR") to the Financial Intelligence Unit.

8.10 The nominated officer must decide, independently, if they suspect that the customer is engaged in money laundering. A separate offence is committed if the nominated officer suspects money laundering and does not make the required disclosure to the UK Financial Intelligence Unit as soon as is practicable after the information comes to him or her.

8.11 However, where a nominated officer receives a report of suspicious activity, if they personally are not immediately suspicious, they must consider whether, objectively, there are reasonable grounds to suspect based on the information they have at the time. In our example where the cashier is suspicious, the nominated officer might disagree and elect not to submit a SAR. If the customer was arrested and the cash seized, the police may take the view that there were reasonable grounds to suspect that

---

3 As discussed in Chapter 2, a nominated officer is a person who is nominated within a firm, company or other organisation to submit suspicious activity reports on their behalf.

4 Proceeds of Crime Act 2002, s 330.

5 Proceeds of Crime Act 2002, s 330.

6 PNC Statistics (2013 to 2016) provided by National Police Chiefs' Council.

7 As per Proceeds of Crime Act 2002, s 330(4).

they were engaged in money laundering. Whilst the cashier had discharged their obligation to disclose, the nominated officer could be prosecuted under section 331 for failing to make a required disclosure. Between 2013 and 2016, 12 cases were prosecuted to trial under section 331 of the Proceeds of Crime Act 2002. There were a further 158 cases which resulted in a criminal investigation but did not proceed to a trial.[8]

8.12 We will now consider how the thresholds of suspicion and reasonable grounds to suspect have been applied in practice in relation to sections 330 and 331 of the Proceeds of Crime Act 2002 as well as suspicion thresholds used in other jurisdictions.

The threshold of the offences

The meaning of "suspects"

8.13 We have already considered the meaning of "suspicion" and its derivations in detail in Chapter 6. We will now examine how suspicion has been interpreted in the context of reporting obligations in European law and in other jurisdictions.

European approach to suspicion in context of reporting obligations

8.14 There has been no definitive guidance from the Court of Justice of the European Union (CJEU) on the meaning of the terms "suspect" or "reasonable grounds to suspect" as they appear in the Fourth Money Laundering Directive ("4AMLD").

8.15 Suspicion has been considered by the European Court of Human Rights in the context of reporting offences. In *Michaud v France,*[9] the European Court of Human Rights considered the meaning of suspicion in the context of reporting obligations under domestic law based on the provisions of the First, Second and Third Money Laundering Directives. The Court referred to suspicion as a matter of "common sense". It is of note that the Court referred to the availability of specific guidance in the Monetary and Financial Code for reporters,[10] however, as in the UK, there is no legal definition of suspicion (or "good reason to suspect").[11] Guidance provided by the Autorité des Marchés Financiers (AMF) (which regulates participants and products in France's financial markets) states:

> There is no legal definition of suspicion. To understand the term "suspect", it could be helpful to refer to the interpretation of the Conseil d'Etat in its Judgment of 31 March 2004, which was handed down under the old regulations. This judgment states that, if the information gathered by an investment undertaking, in accordance with due diligence under the applicable regulations, does not let the undertaking rule out any suspicion about the lawfulness of the transaction or the origin of the sums involved,

---

8 PNC Statistics (2013 to 2016) provided by National Police Chiefs' Council.

9 Application no. 12323/11, judgment 6 December 2012.

10 http://www.amf-france.org/en_US/Reglementation/Doctrine/Doctrine-list/Doctrine?docId=workspace%3A%2F%2FSpacesStore%2F3513a5da-b7dd-4c1a-8dde-0ba7909a8dcb&category=III+-+Providers (last accessed 29 June 2018).

11 See Autorite Des Marches Financiers, *Guidelines on the obligation to report suspicious transactions to TRACFIN* (2010), p 5.

and thus rule out the possibility that these sums are the proceeds of an underlying offence, it must file a report with Tracfin.[12]

8.16 The Court of Justice of the European Union has also considered the meaning of suspicion within the context of the Third Money Laundering Directive. In *Safe Interenvios, SA v Liberbank, SA*[13], a preliminary ruling was sought by the Audiencia Provincial de Barcelona (Spain) on a matter of law from the Court of Justice of the European Union. The issue in the case was whether the Third Money Laundering Directive precluded a Member State from authorising a credit institution to apply customer due diligence measures to a payment institution.

8.17 Advocate General Sharpston observed in an Opinion that Article 22(1)(a) (on the scope of the obligation to report to the Financial Intelligence Unit ("FIU")) suggested that suspicion was not the same as having 'reasonable grounds to suspect.' However, AG Sharpston concluded that suspicion (in relation to Article 7 of Directive 2005/60) could not be a purely subjective matter:

> The Money Laundering Directive does not define 'suspicion of money laundering or terrorist financing'. Although Article 22(1)(a) (on the scope of the obligation to report to the FIU) suggests that having 'suspicion' is not the same as having 'reasonable grounds to suspect' that money laundering or terrorist financing is being (or has been) committed or attempted. I consider that that distinction cannot be read to mean that 'suspicion' in Article 7(c) is a purely subjective matter. In my opinion, suspicion must be based on some objective material that is capable of review in order to verify compliance with Article 7(c) and other provisions of the Money Laundering Directive. Thus, in my opinion, 'a suspicion of money laundering or terrorist financing' within the meaning of Article 7(c) of Directive 2005/60 arises in particular where, taking into account the individual circumstances of a customer and his transactions (including with respect to the use and management of his account(s)), there are some verifiable grounds showing a risk that money laundering or terrorist financing exists or will occur in relation to that customer.[14]

8.18 This interpretation endorses an evidence-based approach to suspicion. The difference between requiring the existence of some verifiable grounds and requiring "reasonable grounds for suspicion" is perhaps a matter of degree. The Court (5th Chamber) in the same case did not offer any interpretation of suspicion, which was not in issue in the case, and stated that "a suspicion of money laundering or terrorist financing" was not a concept defined in the Directive.[15]

---

12 Autorite Des Marches Financiers, *Guidelines on the obligation to report suspicious transactions to TRACFIN* (2010).

13 Opinion of Advocate General Sharpston, Case C-235/14 Safe Interenvios, SA v Liberbank, SA; Banco de Sabadell, SA and Banco Bilbao Vizcaya Argentaria, SA Official Journal of the European Union, C 235, Vol. 57, 21 July 2014.

14 Opinion of Advocate General Sharpston, Case C-235/14 Safe Interenvios, SA v Liberbank, SA; Banco de Sabadell, SA and Banco Bilbao Vizcaya Argentaria, SA Official Journal of the European Union, C 235, Vol. 57, 21 July 201, para 128.

15 Case C-235/14, 10th March 2016.

8.19 In the following section, we will examine the Canadian model of reporting suspicious activity which is based on the threshold of "reasonable grounds to suspect". The Canadian approach appears to require a reporter to have a subjective suspicion which is based on objective grounds. This accords more closely with the approach of the House of Lords in *R v Saik*.[16]

The meaning of "reasonable grounds for suspecting"

8.20 As we observed in Chapter 6, sections 330(2) and 331(2) of the Proceeds of Crime Act 2002, which apply to the regulated sector, require that the person "(a) knows or suspects, or (b) has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering."

8.21 In contrast, section 332 of the Proceeds of Crime Act 2002, which applies to nominated officers outside the regulated sector, omits "reasonable grounds for knowing or suspecting". Instead, it requires that the person "know or suspect" that another person is engaged in money laundering.

8.22 As there has been no definitive judgment to date on the meaning of "reasonable grounds for suspecting" in the context of sections 330 and 331 of POCA, there are two possible interpretations to consider. We will examine both of these possible interpretations in the next section of this Chapter.

Is "reasonable grounds to suspect" a cumulative test?

8.23 In Chapter 6, we discussed the interpretation of "reasonable grounds to suspect" in *R v Saik.*[17] The House of Lords held that the phrase "reasonable grounds to suspect" amounted to a cumulative test with a subjective and an objective element. It required a subjective suspicion based on objective grounds.

8.24 In contrast to the legislative provision that was considered in *R v Saik*, sections 330 and 331 of the Proceeds of Crime Act 2002 use four different terms: "know", "suspect", "reasonable grounds to know and "reasonable grounds to suspect". This creates four separate ways of committing an offence under section 330 or 331 of POCA.

8.25 If, subsection (2)(b) is to be interpreted in accordance with *R v Saik*, then it would appear to make the term "suspect" redundant as subjective suspicion would be subsumed within "reasonable grounds to suspect".

8.26 Whilst "reasonable grounds to suspect" has not been interpreted by the courts in the context of sections 330 and 331 of POCA, "reasonable cause to suspect has been addressed in the context of the Terrorism Act 2000 by the Supreme Court in the recent case of *R v Sally Lane and John Letts.*[18] In the course of the judgment, the Court referred to section 21A of the Terrorism Act, the language of which mirrors sections 330

---

16 [2006] UKHL 18; [2007] 1 AC 18.

17 [2006] UKHL 18; [2007] 1 A C 18.

18 [2018] UKSC 36.

and 331. Section 21A uses the terms "knows, suspects, or has reasonable grounds for knowing or suspecting". Lord Hughes stated:

> In that section, or any other similarly constructed, it is plain beyond argument that the expression "has reasonable grounds for suspicion" cannot mean "actually suspects".[19]

8.27 If this is applied to sections 330 and 331, this would confirm that "reasonable grounds to suspect" is a wholly objective test within the context of the disclosure offences.

Reasonable grounds to suspect: the Canadian approach

8.28 In Canada, reasonable grounds for suspicion is the threshold for reporting obligations. The Federal Court of Appeal has considered the meaning of "reasonable grounds to suspect" in an investigative context. In *Sellathurai v Canada*[20], the Court considered the term in the context of a legislative provision authorising the seizure of the cash if there were reasonable grounds to suspect that the funds were the proceeds of crime. The Court upheld the application judge's approach to the term requiring objective evidence to support a subjective suspicion:

> The application Judge analysed the issue of the standard of proof that is required to establish reasonable grounds to suspect. She found that there must be more than a mere subjective suspicion. Instead, the application Judge found that to substantiate reasonable grounds to suspect, there must be objective and credible evidence. This finding of the application Judge is consistent with the conclusion of the Supreme Court of Canada in its recent decision in *R v Kang Brown, [2008] 1 S.C.R. 456*. In that case the standard of proof that is required to establish a "reasonable suspicion" is described, in paragraph 75, as one that requires objectively ascertainable facts that are capable of judicial assessment. In my view there is little to differentiate a "reasonable suspicion" from "reasonable grounds to suspect". Accordingly, I am of the view that the standard of proof described in Kang-Brown is an appropriate one to be applied to the determination of whether reasonable grounds to suspect may be said to exist. I would hasten to add that I see no material difference between that standard of proof and the standard of proof as formulated by the application Judge.

8.29 Therefore there is some basis to suggest that "reasonable grounds to suspect" requires both a subjective suspicion and an objective, evidence-based foundation for the suspicion. The Canadian approach provides a useful insight into how a cumulative test works in p0ractice in the context of money laundering reporting obligations, and is worth considering in more detail.

8.30 The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) was established under section 41 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2000. FINTRAC's purpose is to facilitate the detection and prevention of money laundering and terrorist financing. FINTRAC collects and analyses information obtained from financial transactions and oversees compliance by the reporting sectors.

---

19 [2018] UKSC 36, para 22.

20 [2009] 2 FCR, paras 111 to 112.

8.31 Suspicious transactions are defined as financial transactions which the reporter has reasonable grounds to suspect are related to the commission of a money laundering offence or a terrorist financing offence. Therefore, the reporting threshold is set at "reasonable grounds to suspect".[21] In relation to the money laundering offences, the threshold is set at knowledge or belief.[22]

8.32 Whilst suspicion is not defined, guidance to reporters provides that what constitutes "reasonable grounds to suspect" is determined by what is reasonable "in your circumstances, including normal business practices and systems within your industry." Canadian reporters are provided with guidance on interpreting and applying the test of reasonable grounds for suspicion, including lists of general and industry-specific indicators for money laundering and terrorist financing. These lists have been compiled with input from industry, law enforcement agencies and FINTRAC. [23]

8.33 In particular, the guidance states that:

> A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. As a general guide, a transaction may be connected to money laundering or terrorist activity financing when you think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust...
>
> An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. Remember that behaviour is suspicious, not people. Also, it could be the consideration of many factors–not just one factor–that will lead you to a conclusion that there are reasonable grounds to suspect that a transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. All circumstances surrounding a transaction should be reviewed.

8.34 The indicators of money laundering include lists of factors to be considered under different headings. For example, there is a list of general factors, a list of indicators of money laundering which relate to an individual's identity and specific factors to be considered where a cash transaction is involved. They range from common-sense

---

21 Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), s.7 requires regulated entities to report to FINTRAC every financial transaction that occurs, or that is attempted, in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an money laundering or terrorist financing offense. https://www.canlii.org/en/ca/laws/stat/sc-2000-c-17/latest/sc-2000-c-17.html?searchUrlHash=AAAAAQA-cHJvY2VlZHMgb2YgY3JpbWUgbW9uZXkgbGF1bmRlcmluZyBhbmQgdGVycm9yaXN0IGZpbmFuY2luZyBhY3QAAAAAAQ&resultIndex=4 accessed on 29 May 2018. See also Financial Action Task Force, Anti-money laundering and counter-terrorist financing measures: Canada Mutual Evaluation Report at http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf accessed on 28 May 2018.

22 See Canadian Criminal Code, ss 354 (possession of proceeds), 355.2 (trafficking in proceeds), and 462.31 (laundering proceeds).

23 FINTRAC, Guideline 2 Suspicious Transactions, (2017) para 7. http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp#s3-1,

practical points to specific actions or behaviours indicative of a particular money laundering practice. They include some of the following examples:

(1) A client does not want correspondence sent to his or her home address;

(2) A client insists a transaction be executed quickly;

(3) A transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist);

(4) A reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.[24]

8.35 Schedule 1, Part G requires reporters to give a detailed description of the grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering offence or terrorist financing activity. The Regulations set out, in detail, the specific information required to fulfil the disclosure obligation.

8.36 This approach seems appropriate in a reporting context, providing an additional safeguard for those who are the subject of a disclosure. The clear guidance benefits reporters by identifying and articulating what would constitute reasonable grounds for a suspicion.

Is "reasonable grounds to suspect" an objective test?

8.37 Hansard reports demonstrate that during the debates on the Proceeds of Crime Bill, the disclosure offences were intended to include a wholly objective test for criminality. This was intended to encourage the financial industry to be much more diligent in reporting suspected money laundering.[25] It was considered reasonable to expect a higher level of care from employees in the regulated sector who are reporting suspicious financial transactions.[26]

8.38 The inclusion of sub-sections (2)(b) in sections 330 and 331 has been the subject of commentary concerning the breadth of the offences under those sections. Miriam Goldby also argues that section 330(2)(b) create an objective test which establishes liability for negligence:

> …liability for breach of section 330 may arise not only where a person knows or suspects and does not file a SAR, but also where a person should have known or suspected, as there were reasonable grounds to do so. This introduces an objective test of liability.[27]

---

24 FINTRAC, Guideline 2 Suspicious Transactions, para 8. http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp#s3-1. (last Accessed on 28 May 2018).

25 Hansard, Official Report, Standing Committee B, col.1070 (January 22, 2002).

26 Part VIII, para. 8.6, Proceeds of Crime Consultation on Draft Legislation. Cm 5066.

27 Miriam Goldby, Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform, [2013] Journal of Business Law 367, p 371.

8.39 If it is a purely objective test, it is sufficient for the prosecution to prove either that the defendant actually suspected or that there were reasonable grounds to suspect the relevant facts.[28] Under those circumstances sections 330(2)(b) and 331(2)(b) would be satisfied if, objectively determined, a defendant had reasonable grounds for suspecting money laundering notwithstanding that he did not actually hold that suspicion. This interpretation has yet to be tested by the appellate courts.

8.40 Other jurisdictions have similarly upheld objective tests in the context of criminal offences. In *HKSAR v Shing Siu Ming*,[29] the applicants were convicted of drug trafficking offences. One of the issues at trial was whether the offender knew or had reasonable grounds to believe that the person to whom assistance was given had been a drug trafficker or had benefited from drug trafficking. In contrast to the UK approach in *Saik*[30], the Court of Appeal (HK) held that the prosecution was not called upon to prove *actual* belief:[31]

> In our view it requires proof that there were grounds that a common sense, right-thinking member of the community would consider were sufficient to lead a person to believe that the person being assisted was a drug trafficker or had benefited therefrom. That is the objective element. It must also be proved that those grounds were known to the defendant. That is the subjective element.[32]

8.41 It is relevant to note that in *A-G of Hong Kong v Lee Kwong-Kut* (1993)[33] the UK Privy Council considered section 25 of the Drug Trafficking (Recovery of Proceeds) Ordinance (HK), which was similar to section 24 of the UK Drug Trafficking Offences Act 1986 (entering into an arrangement). However, the *mens rea* element of the former

---

28 *Smith, Hogan, and Ormerod's Criminal Law* (2018) 3.2.8.2 at fn 232.

29 Power VP, Mayo and Stuart-Moore JJA [1999] 2 HKC 818 at 825, applying the old Drug Trafficking (Recovery of Proceeds) Ordinance.

30 *R v Saik (Abulrahman)* [2006] UKHL 18; [2007] 1 A C 18.

31 Power VP, Mayo and Stuart-Moore JJA [1999] 2 HKC 818 at 825, applying the old Drug Trafficking (Recovery of Proceeds) Ordinance at para 48.

32 See also HKSAR v. Pang Hung Fai [2014] HKCFA 96; (2014) 17 HKCFAR 778; [2014] 6 HKC 487; FACC 8/2013 (10 November 2014), HKSAR v Yeung Ka Sing, Carson [2016] HKCFA 53; (2016) 19 HKCFAR 279; FACC 6-2015, Yan Suiling (2012) 15 HKCFAR 146.

33 [1993] A C 951, [1993] 3 W.L.R. 329. At the time that this case was decided, section 25 of the Drug Trafficking (Recovery of Proceeds) Ordinance (Laws of Hong Kong, 1989 rev., c.405) provided: "(1) Subject to subsection (3), a person who enters into or is otherwise concerned in an arrangement whereby - (a) the retention or control by or on behalf of another ('the relevant person') of the relevant person's proceeds of drug trafficking is facilitated (whether by concealment, removal from the jurisdiction, transfer to nominees or otherwise); or (b) the relevant person's proceeds of drug trafficking - (i) are used to secure that funds are placed at the relevant person's disposal; or (ii) are used for the relevant person's benefit to acquire property by way of investment, knowing or having reasonable grounds to believe that the relevant person is a person who carries on or has carried on drug trafficking or has benefited from drug trafficking, commits an offence..... (3) Where a person discloses to an authorised officer a suspicion or belief that any funds or investments are derived from or used in connection with drug trafficking or any matter on which such a suspicion or belief is based - (a) if he does any act in contravention of subsection (1) and the disclosure relates to the arrangement concerned, he does not commit an offence under this section if the disclosure is made in accordance with this paragraph, that is - (i) it is made before he does the act concerned, being an act done with the consent of the authorised officer; or (ii) it is made after he does the act, but is made on his initiative and as soon as it is reasonable for him to make it...."

was "*knowing or having reasonable grounds to believe* that the relevant person is a person who carries on or has carried on drug trafficking or has benefited from drug trafficking, commits an offence". Their Lordships remarked that this mental element can exist "even if the defendant does not have the required belief, if there are reasonable grounds for his holding the belief. The offence is therefore a Draconian one" (per Lord Woolf).[34] The decision of the Privy Council in *Lee Kwong-Kut* pre-dates *R v Saik*.[35]

8.42 The comments of Lord Hughes in *R v Sally Lane and John Letts* put beyond doubt that "reasonable grounds to suspect" in sections 330 and 331 would be interpreted as an objective test were it to come before the Court.[36] This accords with how the test is applied in practice. From the limited evidence we have available, "reasonable grounds to suspect" has been applied as an objective test. There have been a relatively small number of prosecutions under the disclosure offences.[37]

8.43 In those cases that have been reported, it has been accepted at first instance, either by the jury's verdict on direction from the trial judge or a plea of guilty, that "reasonable grounds to suspect" is an objective test in the context of section 330 of the Proceeds of Crime Act 2002.

8.44 In *R v Swan*[38], the applicant had pleaded guilty to an offence under section 330 of the Proceeds of Crime Act 2002 on the "reasonable grounds to suspect" limb of the test. She had been responsible for day-to-day operations for a company dealing with safe deposit boxes. Undercover police officers had made "test purchases" which "revealed that the facilities were being made available to anyone who wished to use them for what were obviously suspicious and potentially criminal activities." The applicant had pleaded guilty on the basis she had reasonable grounds to suspect in each case that the undercover officers and holders of the boxes were engaged in money laundering, she did not actually know or suspect that that was the case (although she did accept that she had reasonable grounds for suspecting). The matter came before the Court of Appeal in respect of sentence and no issue was taken with the basis of plea.

8.45 In *R v Griffiths,*[39] the appellant was a solicitor who had undertaken a conveyancing transaction in relation to a property owned by drug dealers. He had been acquitted of a money laundering offence under section 328 of the Proceeds of Crime Act 2002, but was convicted of failing to make a required disclosure under section 330. The prosecution accepted that the appellant had not known or suspected that persons were engaged in money laundering. Rather the appellant had reasonable grounds to suspect. The house had been sold at a significant undervalue yet the transaction had been carried out for a normal conveyancing fee.

---

34 [1993] A C 951, at page 964 paras G to H.

35 [2006] UKHL 18; [2004] EWCA Crim 2936.

36 [2018] UKSC 36, para 22.

37 Between 2013 and 2016 there were 1,416 prosecutions under s 330 POCA, 170 under s 331 and 60 under s 332: Police National Computer Statistics provided by the National Police Chiefs' Council (April 2018).

38 [2011] EWCA Crim 2275; [2012] 1 Cr App R (S) 90.

39 [2006] EWCA Crim 2155; [2007] 1 Cr App R (S) 95.

8.46 In summary, it is strongly arguable that "reasonable grounds for suspecting" is a wholly objective test in the context of sections 330(2)(b) and 331(2)(b) of the Proceeds of Crime Act 2002.

The implications of the current threshold: "suspects" or "has reasonable grounds for suspecting"

8.47 If, as we have set out above, the addition of "reasonable grounds for suspecting" introduces a purely objective test then it significantly broadens the scope of the disclosure offences under section 330 and 331. There is no additional layer of protection for reporters which would otherwise be provided by a cumulative test as in *R v Saik*.[40]

8.48 At their broadest, these provisions may criminalise not only those who know or suspect that money laundering is taking place and who fail to pass that information to the authorities, but those who may not have noticed what a court might regard, with hindsight, as grounds to suspect that money laundering was taking place. As Goldby observes, if the reasonable person would have suspected money laundering but the reporter did not, the reporter may still be criminally liable.[41]

8.49 The justification for an objective threshold in this context is that an employee or professional in the regulated sector trained to spot behaviour indicative of money laundering should be blameworthy for their failure to report.[42] Ashworth and Horder identify four key features that justify the use of a negligence standard in a criminal offence:

(1) the potential harm is great: money laundering is a direct threat to the integrity of the financial system and perpetuates an ongoing cycle of crime. In addition, terrorist financing represents a risk of direct harm to members of the public;

(2) the risk of the laundering occurring is obvious: the risk of money laundering/terrorist financing should be obvious to an employee in the regulated sector who is experienced at dealing with financial transactions;

(3) The cashier and nominated officer have a duty to try to avoid the risk: given the scope of the regulated sector, the nature of the transactions that they are involved in and the wider responsibility to the public to prevent criminal transactions, this requirement can be justified;

(4) The cashier and nominated officer have the capacity to take the required precautions: banks and businesses operating in the regulated sector are required to put systems in place to detect money laundering. These include conducting customer due diligence checks and enhanced measures where greater risk is identified. Staff within a bank or business in the regulated sector are subject to

---

40 *R v Saik* [2006] UKHL 18, [2006] 2 WLR 993.

41 Miriam Goldby, Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform, [2013] *Journal of Business Law* 367, p 372.

42 See H L A Hart 'Negligence, Mens Rea, and Criminal Responsibility.' In *Punishment and Responsibility* 136-157. If an individual had the capacity and a fair opportunity to make the right choice, they can be blameworthy for their failure to make the right choice.

specialist training to assist with the identification and reporting of suspicious activity.[43]

8.50 Applying this criteria to money laundering, this analysis provides some support for the case for the threshold to remain at "suspects" or "reasonable grounds for suspecting" applied to money laundering and terrorism financing.

8.51 There are three important safeguards aimed at protecting employees, which, to some extent, mitigate the potentially draconian breadth of these provisions:

(1) a defence of reasonable excuse is available;[44]

(2) the Court is obliged to have regard to any (HM Treasury approved) sector specific guidance in determining whether an offence has been committed;[45]

(3) a specific defence of lack of training by an employer is available to those subject to such a charge.[46]

8.52 There is also an additional evidential burden on the prosecution. Corker argues that the prosecution must prove the information constituting reasonable grounds was, at the material time, actually known to the accused. This is based on the legislative requirement that the information must have come to an individual 'in the course of business in the regulated sector.' This is a higher threshold that proving than the information was merely available or accessible to him.[47]

8.53 There are also legitimate policy arguments in favour of imposing criminal liability based on an objective test. This desired deterrent effect was referred to in the explanatory notes to the original Proceeds of Crime Bill.[48] The Government concluded that the introduction of a "negligence test" was necessary as a deterrent against those in the financial sector and other regulated sectors who fail to act competently and responsibly where information before them ought to make them suspect money laundering. In addition to the high level of care expected from employees in the regulated sector, the risk of harm to the integrity of the financial system would be substantial if money laundering were to go undetected. It is worth noting that there was significant debate during the Bill's passage on whether a wholly objective test was justified.[49]

---

43 Andrew Ashworth and Jeremy Horder, *Principles of Criminal Law* (7th edition 2013) at page 184.

44 Proceeds of Crime Act s 330(6)(a).

45 Proceeds of Crime Act s 330(8).

46 Proceeds of Crime Act s 330(7).

47 https://www.corkerbinning.com/failure-to-disclose-does-not-equate-to-negligence/ (last accessed 4 June 2018).

48 Home Office, Proceeds of crime: consultation on draft legislation at pages 300 to 301.

49 See for example the debate concerning a proposed amendment which would have created two separate and distinct offences and reduced the penalty for negligent failure to disclose to a fine not exceeding level 5 on the standard scale. Hansard HC Deb, 27 February 2002, column 715. Amendment No. 175 in clause 332. Level 5 would allow for an unlimited fine in accordance with Criminal Justice Act 1982, s 37(2) and Legal Aid, Sentencing and Punishment of Offenders Act 2012, s 85(1).

8.54 However, there are other impacts to consider. An objective test lowers the threshold of criminality below subjective suspicion. This may have a consequential effect on the volume and quality of required disclosures. Goldby argues that the objective standard to which reporters are held drives defensive reporting as it promotes over-caution. It may discourage the reporter from exercising their judgment or realistically evaluating the risk.[50]

> …the main problem with section 330 [of the Proceeds of Crime Act 2002] is that it encourages the reporting of any and every suspicion no matter how small and insignificant. It does not therefore do much towards encouraging the implementation of a truly risk-based approach.

8.55 In practical terms, Campbell argues that the danger inherent in criminal sanctions in this context is over-reporting, meaning those in the regime are "drowned in data", with questionable benefit.[51]

8.56 The scope and fairness of the offence when taken as whole must also be considered. The question of whether the prosecution must prove that actual money laundering occurred in order to secure a conviction under sections 330 to 332 of POCA remains unresolved. There has been no definitive appellate judgment on the issue.

8.57 During the second reading of the Bill in the House of Lords, Lord Goldsmith (then Attorney General) attempted to placate concerns over the breadth of the offence by noting that a prosecution could only proceed if the agency could prove money laundering was in fact planned or undertaken:

> The concern that the negligence offence is unfair overlooks the fact that the offence in clause 330 of failing to report to the authorities is permitted only if the prosecution proves that money laundering was planned or undertaken.[52]

8.58 However, this issue has been argued before the High Court of Justiciary and an alternative view was taken of the effect of the provision. In *Ahmad v HM Advocate*[53], a Scottish case, the appellant was convicted under section 330(1) POCA for failing to make a required disclosure (under section 330(5)) of known or suspected money laundering. The appellant was the secretary, director and 50% shareholder of a travel agency and money service bureau that received deposits of “unexplained quantities of cash”. In the High Court of Justiciary, it was argued by the appellant that the Crown must prove that money laundering actually occurred in order for the jury to convict. The Court was unimpressed by this argument:

---

50 Miriam Goldby, *Anti-money laundering reporting requirements imposed by English law: measuring effectiveness and gauging the need for reform*, [2013] Journal of Business Law, p 373.

51 Liz Campbell, *Dirty cash (money talks): 4AMLD and the Money Laundering Regulations 2017* [2018] Crim LR 102 at 107.

52 HL Deb 25 March 2002: Column 62 https://publications.parliament.uk/pa/ld200102/ldhansrd/vo020325/text/20325-10.htm (last accessed 4 June 2018).

53 [2009] HCJAC 60; 2009 S L T 794; 2009 S C L 1093; 2009 S C C R 821; [2010] Lloyd's Rep F C 121

> There is nothing in the language of section 330(2) which states or requires that money laundering is in fact taking place. It is plain that the obligation thereunder can arise if a person suspects or has reasonable cause for suspecting that it is. Given that the apparent purpose of the section is to prevent money laundering and in particular to provide assistance to the investigatory authorities, so that they may investigate, it is not obviously consistent with that purpose to require proof of actual money laundering. If the Crown were required to prove actual money laundering at the time when the relevant suspicion arises (as was argued by senior counsel) it is not difficult to imagine considerable practical difficulty, given that it is only thereafter that investigation, prompted by the reporting, may be expected to begin, and evidence obtained. Moreover, the effect of the appellant's contention is, in our view, to require an additional condition where none is specified.

8.59 As this issue has not yet been argued in the English appellate courts, it is unclear whether the prosecution would be required to prove that money laundering had occurred in order to secure a conviction under sections 330-332. *Ahmad*[54] sets out a convincing argument that proof of money laundering is not required. If this is the case, and the additional layer of protection envisaged by the House of Lords in *R v Saik*[55] is absent, it raises the question of fairness. Employing the broadest interpretation, sections 330 and 331 of the Proceeds of Crime Act 2002 may capture a failure to disclose where the reporter did not suspect, but there were reasonable grounds to suspect despite the fact that no money laundering had in fact occurred. It is not clear that the conviction of a defendant under these circumstances would be fair or desirable as a matter of policy.

8.60 It is strongly arguable therefore, that the objective test sets the threshold for liability too low. In the next Chapter, we will examine the case for reforming the thresholds of suspicion in Part 7 of the Proceeds of Crime Act 2002 and the options to be considered.

---

54 [2009] HCJAC 60; 2009 S L T 794; 2009 S C L 1093; 2009 S C C R 821; [2010] Lloyd's Rep F C 121

55 *R v Saik* [2006] UKHL 18, [2006] 2 WLR 993.

Chapter 9: The case for reforming the suspicion threshold

9.1 We have examined a number of different approaches to the interpretation of the concept of suspicion in the preceding Chapters. The term encompasses a hierarchy of states of mind of differing strength and conviction, frequently depending on the context in which the term is used.

9.2 Suspicion can range from:

(1) imagining something without evidence;

(2) a possibility, which is more than fanciful, that the relevant facts exist;[1]

(3) suspicion on some verifiable or articulable grounds;[2]

(4) having a strong or settled suspicion that is firmly grounded and targeted on specific facts.[3]

9.3 In the next section, we will consider whether the concept of suspicion should be defined, and whether there is a need for statutory guidance to assist reporters on its application. We will go on to consider the merits of placing greater reliance on the alternative threshold of "reasonable grounds to suspect" in the context of Part 7 of the Proceeds of Crime Act 2002. We will also examine whether the thresholds of suspicion for the money laundering offences and the disclosure offences are appropriate and work effectively. Finally, we will outline how the threshold for required and authorised disclosures might be reformed to strike a better balance and improve effectiveness as between the interests of law enforcement agencies, reporters and those who are the subject of a disclosure.

Should suspicion be defined?

9.4 As we have described in the preceding chapters the ordinary meaning of suspicion is wide, and is being interpreted in a variety of ways. This lack of clarity may be contributing to defensive reporting, and even the inadvertent commission of offences. One solution to this problem might be to define suspicion in the Proceeds of Crime Act 2002.

9.5 We looked in some detail at the ordinary meaning of suspicion and the courts' approach to suspicion in the preceding chapters. Taking into account the approach to ordinary

---

1 *R v Da Silva* [2006] EWCA Crim 1654, [2007] 1 W L R 303.

2 Opinion of Advocate General Sharpston, Case C-235/14 Safe Interenvios, SA v Liberbank, SA; Banco de Sabadell, SA and Banco Bilbao Vizcaya Argentaria, SA Official Journal of the European Union, C 235, Vol. 57, 21 July 2014.

3 *Manifest Shipping Co Ltd v Uni-Polaris Insurance Co Ltd* [2003] 1 AC 469.

English words in *Brutus v Cozens*[4], *Saik*[5] and *Da Silva*[6], it is clear that in principle an ordinary English word should only be defined where it is to be qualified in some way or given special meaning. On this basis it is strongly arguable that it would be undesirable to define suspicion.

9.6 Putting aside issues of principle, there are considerable practical difficulties in formulating a precise and workable legal definition which would add anything to the ordinary, natural meaning. It is difficult to envisage any way to articulate the essence of suspicion that would usefully encompass all of the various ways of expressing suspicion that we examined above.

9.7 However, we invite consultees' views on whether suspicion should be defined for the purposes of Part 7 of the Proceeds of Crime Act 2002 and, if so, what that definition might look like. Is there a definition which is preferable to that adopted in *R v Da Silva*?[7]

Consultation Question 2.

9.8 We would value consultees' views on whether suspicion should be defined for the purposes of Part 7 of the Proceeds of Crime Act 2002? If so, how could it be defined?

Would guidance improve the application of suspicion by the reporting sector?

9.9 Without necessarily making any alteration to the threshold for reporting or criminality, nor defining the term in primary legislation, a single source of definitive guidance could improve the application of the suspicion threshold by reporters. The *Da Silva* interpretation arguably confirms that a suspicion should have some foundation otherwise it would be rejected as a "mere inkling". Guidance to reporters could identify and catalogue those grounds or factors which may raise a suspicion and promote greater consistency in application.

9.10 Such guidance on suspicion could assist in ensuring that the maximum value of SARs intelligence is exploited. The National Crime Agency screens and analyses SARs using specific key words.[8] The search terms could be based on the language of any guidance that is produced. Similarly, if reporters tailored their reports using key words to reflect the guidance, this common format would help to encourage a common understanding of what suspicion means. That would assist both the NCA and law enforcement agencies to perform key word searches and conduct data analysis to greater effect. The combination of a prescribed form which requires articulated grounds accompanied by guidance setting out as clearly as possible what those grounds might be would achieve

---

4 (1972) 56 Cr App R 799 at 804.

5 [2006] UKHL 18, [2007] 1 AC 18.

6 [2006] EWCA Crim 1654, [2007] 1 W.L.R. 303.

7 [2006] EWCA Crim 1654, [2007] 1 W.L.R. 303.

8 National Crime Agency, Suspicious Activity Reports Annual Report (2017) p 11.

greater uniformity in the reports enabling both the NCA and law enforcement agencies to ascertain more quickly the nature of the suspicion.

9.11 Such guidance should also make it much easier for supervisory authorities to educate and advise their members. It would resolve to some extent the problem of inconsistent guidance on the law between different supervisory authorities.

9.12 We provisionally propose that guidance on suspicion should be issued. There are strong arguments to suggest that this will improve the quality of reporting, reduce the number of unnecessary or poor-quality reports and lead to greater consistency. Ideally, that guidance should identify (in a non-exhaustive list) those factors capable of founding a suspicion (or reasonable grounds for suspicion if that course is adopted as discussed below) and those which should be excluded. We believe that consulting with stakeholders during the drafting of the guidance will ensure that it is comprehensive and useful.

9.13 For this proposal to have maximum effect we propose that it should be formal guidance from Government issued under a statutory power, rather than industry guidance or a general circular from a Government department.

9.14 At this stage, we make no more specific proposals regarding *how* this guidance should be issued but we offer three examples for consideration. Under the Police and Criminal Evidence Act (PACE) 1984, the Codes of Practice are central to maintaining the right balance between the powers of the police and the rights and freedoms of the public. These Codes of Practice have been revised regularly to account for changing circumstances and provide guidance on principle as well as practical assistance in applying the legislation fairly and consistently. Section 67(4) of PACE requires that where the Home Secretary wishes to revise a Code of Practice, a statutory consultation must first be carried out. This consultation must include specified stakeholders and other persons as the Home Secretary thinks fit.

9.15 The Bribery Act 2010 may also provide a model for consideration. The Act creates an offence under section 7 which can be committed by commercial organisations which fail to prevent persons associated with them from committing bribery on their behalf. It is a full defence for an organisation to prove that despite a particular case of bribery being committed by an associate it nevertheless had adequate procedures in place to prevent persons associated with it from bribing. Section 9 of the Act requires the Secretary of State to publish guidance about procedures which commercial organisations can put in place to prevent persons associated with them from bribing. The objective of this guidance is to provide assistance concerning procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing. The guidance is designed to be of general application and includes commentary and examples.

9.16 A further example can be found in relation to the Criminal Finances Act 2017. HM Revenue and Customs have issued guidance on the corporate offences of failure to prevent the criminal facilitation of tax evasion.[9] This guidance explains the policy behind

[9] HMRC, Tackling tax evasion: government guidance for the corporate offences of failure to prevent the criminal facilitation of tax evasion, (1st September 2017)

the creation of these new offences and offers assistance on how corporations can institute proportionate procedures to prevent the commission of a criminal offence.

9.17 We invite consultees to consider whether statutory guidance should be issued to assist reporters on the issue of suspicion.

Consultation Question 3.

9.18 We provisionally propose that POCA should contain a statutory requirement that Government produce guidance on the suspicion threshold. Do consultees agree?

Prescribed form

9.19 In conjunction with statutory guidance, we provisionally propose that a prescribed form, or sector specific SAR forms, should be constructed to encourage reporters to articulate evidence-based grounds for a suspicion. This could be done by prescribing the information required for a disclosure in secondary legislation and the form it should take. The Secretary of State already has the power to prescribe the form and manner in which a required or authorised disclosure is made.[10]

9.20 A form, or sector specific SAR forms, designed by a representative panel from the NCA, law enforcement agencies and the various reporting sectors would ensure consistency in the format and presentation of the information in a SAR. Prescribing the information required to constitute a disclosure would ensure that requests for further information diminish over time. In addition, it would make it more difficult for the admittedly small number of reporters who might seek to abuse the authorised disclosure exemption by withholding information. It would also give greater direction to the reporter as to what was required by way of suspicion.

Consultation Question 4.

9.21 We provisionally propose that the Secretary of State should introduce a prescribed form pursuant to section 339 of the Proceeds of Crime Act 2002 for Suspicious Activity Reports which directs the reporter to provide grounds for their suspicion. Do consultees agree?

Consultation Question 5.

9.22 We would welcome consultees' views on whether there should be a single prescribed form, or separate forms for each reporting sector.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf (last accessed on 4 June 2018).

[10] Proceeds of Crime Act 2002, s 339.

The alternative threshold: Saik "reasonable grounds to suspect"

9.23 In this section, we will consider the benefits and disadvantages of adopting the alternative threshold to "suspicion", namely that of "reasonable grounds to suspect" as interpreted in *R v Saik.*[11] We go on to examine whether the current thresholds of simple suspicion for the money laundering offences and "suspects" or "reasonable grounds for suspecting" for the disclosure obligations in Part 7 of the Proceeds of Crime Act 2002 are effective.

9.24 For clarity, we have set out the current thresholds in relation to the money laundering offences in a series of tables below:

Money Laundering Offences **Part 7 POCA 2002**	
Offence	**Current threshold**
Section 327	Knows or suspects
Section 328	Knows or suspects
Section 329	Knows or suspects

Disclosure Offences **Part 7 POCA 2002**	
Offence	**Current threshold**
Section 330	Knows or suspects; or has reasonable grounds for knowing or suspecting
Section 331	Knows or suspects; or has reasonable grounds for knowing or suspecting
Section 332	Knows or suspects

Reporting Obligations **Part 7 POCA 2002**	
Type of Disclosure	**Current threshold**

[11] [2006] UKHL 18, [2007] 1 AC 18.

Required Disclosure (ss 330, 331)	Knows or suspects; or has reasonable grounds for knowing or suspecting
Required Disclosure (s 332)	Knows or suspects
Authorised Disclosure (ss 327(2)(a), 328(2)(a), 329(2)(a))	Knows or suspects

9.25 As we discuss above, a cumulative test requiring proof of subjective suspicion bolstered by objectively reasonable grounds has been used successfully in statutes in relation to investigative powers. The objective limb provides an additional layer of protection. When used in the reporting context, it encourages an evidence based approach to suspicion which protects the subject of the suspicion. We consider that this threshold is an appropriate test in the context of reporting crime.

9.26 Different considerations apply to the threshold for criminal offences. The test requires an offender's suspicion to have an objective foundation which some would argue promotes the interests of fairness. Whilst this cumulative test has been used in the context of criminal offences, it does not necessarily follow that it can be transposed into any criminal offence. In *Pang Hung Fai* (Hong Kong, Court of Final Appeal) [12], the court suggested a cautious approach when applyingsimilar or identical terminology in different contexts:

> This differentiation is a manifestation of the principle of statutory interpretation which focuses on the significance of context, rather than adopting a "natural and ordinary meaning" of particular words. The formulation used to state the mental element of a criminal offence will not necessarily have the same meaning as the same formulation expressed as a description of the state of mind required for the exercise of an executive power. Case law of the latter character, where no issue of mens rea or proof beyond reasonable doubt arises, must be used with considerable circumspection in proceedings of the former character.[13]

9.27 It will depend on the exact nature of the offence as to whether the objective element of the test provides any effective safeguard. That must be balanced against the fact that a cumulative offence may provide an additional barrier to prosecution – albeit a limited one since it is unlikely that a defendant who is found to have a suspicion would be acquitted because he or she did not have reasonable grounds for it. The appropriateness of this test will depend on the context: what the prosecution are required to prove and whether it meets the test of fairness overall.

9.28 In summary, a cumulative test may be more appropriate in an investigative context and in reporting criminal activity. However, it may be less appropriate in the context of a

---

[12] *HKSAR v Pang Hung Fai* [2014] HKCFA 96; (2014) 17 HKCFAR 778; [2014] 6 HKC 487; FACC 8/2013 (10 November 2014).

[13] HKSAR v Pang Hung Fai [2014] HKCFA 96; (2014) 17 HKCFAR 778; [2014] 6 HKC 487; FACC 8/2013 (10 November 2014) at [68].

criminal offence unless the objective element act as a necessary safeguard and does not raise an unnecessary barrier to prosecution.

Adopting a test of reasonable grounds for suspicion in relation to required disclosures

9.29 Requiring "reasonable grounds to suspect" in relation to sections 330 to 331 of POCA (for required disclosures) would introduce a qualitative standard to suspicion importing considerations of strength and cogency.

9.30 One argument against introducing a requirement for suspicion to be based on reasonable grounds is that it could introduce a layer of unnecessary complexity. Whilst is a concept familiar to lawyers, it might prove difficult for individual employees to decide whether or not to report their concerns. This concern could be mitigated by the production of clear guidance and additional training.

9.31 It is also arguable that whilst a police officer conducting normal police investigations should be required to base their suspicion on reasonable grounds,[14] employees in a commercial organisation should not. In *Squirrell v National Westminster Bank,*[15] there was some disquiet about banks being held to the same investigative standard as police officers:

> No doubt it makes sense in relation to the actions of police officers that they should be required to satisfy themselves that reasonable grounds exist for suspecting guilt before they can arrest someone. They have the power and duty to investigate criminal activity. However s 328(1) covers parties like Natwest which have neither the obligation nor the expertise to do so.

9.32 However, we do not consider that to be a compelling argument. In large banks, trained financial investigators are making decisions on disclosure. In any organisation, the nominated officer will have to undergo specific training before performing the role. There are also strong arguments based on the financial impact to an individual or business from an unnecessary disclosure which point towards having a threshold which imports the protections which flow from having to have a reasonable ground to suspect.

9.33 We have considered whether legislation should specify a particular strength of suspicion that would need to be met before a disclosure is made. Penney argues, in the context of Canadian law on police powers, that suspicion standards should be formulated to achieve "reasonable and transparent accommodations between liberty and law enforcement agencies." Penney acknowledges that standards of suspicion can be articulated in many ways but broadly the strength of a suspicion equates to an expression of the probability of those events occurring.[16]

9.34 The strength of a suspicion can be expressed qualitatively (for example, "reasonable grounds for suspicion") or quantitively (an agreed numerical value or range which expresses probability). This "probability threshold" represents the level of confidence in the predicted outcome once it is applied to the facts of the individual case. Following

---

[14] Police and Criminal Evidence Act 1984, s 24 requires reasonable grounds to suspect that an offence has been committed before an arrest can be made.

[15] [2005] EWHC 664 at [15], [2006] 1 WLR 637.

[16] Steven Penney, Standards of Suspicion, Criminal Law Quarterly December 2017, p 24 to 26.

Penney's analysis, having reasonable grounds to suspect a person is engaged in money laundering indicates a greater probability threshold that money laundering has actually occurred than mere suspicion. The reason we can have more confidence in a suspicion supported by objective grounds is that it is evidence-based. As a SAR is an investigative tool, requiring reporters to adopt an evidence-based approach would arguably benefit law enforcement agencies by improving the quality of disclosures so that they actually reflect the probability of money laundering occurring.

9.35 We have also considered the impact that such a change would have on prosecuting criminal cases using the disclosure offences in sections 330 to 332. We do not think that the burden on the prosecution to prove suspicion would be onerous in practice. At trial, a jury would examine whether a defendant's claim that he or she did not suspect money laundering was credible on the basis of the facts known to them and the results of the investigation.

9.36 We consider that that there are strong arguments that the anti-money laundering regime would be improved by raising the threshold for any disclosure from mere suspicion (*Da Silva* suspicion) to "reasonable grounds for suspicion" based on the interpretation in *Saik*.[17] This would mean that the SARs that are filed should be fewer in number and of greater value. In addition, given the potentially serious consequences for the subject of a SAR, it is arguable that those in the regulated sector should be held to a higher standard. The onus should therefore rest on the party making the disclosure to have grounds which are objectively justifiable for doing so.

9.37 Adopting a reasonable grounds to suspect test for the required disclosures under sections 330 to 331 will help to address the problems identified:

(1) disclosure, triggered by suspicion as low as "more than fanciful", risks low value reporting and defensive reporting;

(2) the acknowledgement of defensive reporting by the reporting sector;

(3) increasing numbers of DAML SARs which continue to place pressure on resources of the UKFIU and law enforcement agencies;

(4) the impact of a disclosure on the subject of a SAR which will be exacerbated under an extended moratorium period;

(5) the large disparity in the volume of reports between the UK and other EU countries.

9.38 The Home Office and HM Treasury have indicated that the system needs improvement to ensure that a risk-based approach is embedded allowing reporters to spot criminal activity rather than focus on 'tick-box' compliance.[18] Placing the onus on reporters to demonstrate the objective bases for judgements would be in line with this approach.

---

[17] [2006] UKHL 18; [2007] 1 AC 18.

[18] Joint Home Office and HM Treasury Action Plan for anti-money laundering and counter-terrorist finance (2016) para 1.8.

9.39 In addition, we consider that the reform of the test will be advantageous in relation to the offences created by sections 330 to 331. Taking the scope of those offences at their broadest, there are questions about the fairness of applying a mere suspicion test for criminal liability. This is particularly so if the offences do not require proof that money laundering actually occurred. Removing suspicion in favour of requiring proof of "reasonable grounds to suspect" as interpreted in *Saik*[19] would require reporters to have personal suspicion of money laundering and add an additional layer of protection by establishing that the suspicion is based on some objective grounds. We do not believe that the additional requirement of proving suspicion would be unduly onerous for prosecutors. We also consider that the threshold in section 332 should match 330 and 331 as otherwise the threshold for criminality would be lower for nominated officers operating outside of the regulated sector. In light of the arguments we have made above, there would appear to be no justification for such a distinction.

9.40 We do not, however, propose that any amendment is made in relation to terrorism financing disclosures for two reasons. First, as we outlined in Chapter 3, different considerations apply in cases where terrorism is suspected. Arguably a lower threshold is vital due to the risks of serious harm in the event of a terrorist incident. Secondly, as we observed in Chapter 5, the number of consent SARs which are related to terrorism financing is comparatively low. This creates a clearer divide between the two regimes than currently exists and we invite consultees' views on whether this would create issues in practice.

The relationship between the money laundering offences and authorised disclosures

9.41 Having considered the arguments for requiring reasonable grounds to suspect under sections 330 to 332 before any disclosure is made to the NCA, we must now consider the practical impact of altering the threshold.

9.42 As we discussed in the preceding chapters, whilst required disclosures are triggered by a suspicion or the existence of reasonable grounds to suspect under sections 330 to 332, authorised disclosures are generated in a different way.

9.43 Where a person suspects they are dealing with criminal property and they intend to act in a way that would be prohibited by sections 327, 328 or 329, the authorised disclosure exemption provides protection from criminal liability. In order to amend the threshold for making an authorised disclosure, it would be necessary to amend the threshold for criminality in sections 340 and in sections 327, 328 and 329. Whilst this would achieve the objectives that we have outlined in the preceding paragraphs as regards reporting, it would have other consequences.

9.44 There are strong arguments to retain a pure suspicion threshold for criminality in this context. There is a body of case law surrounding the application of the principal money laundering offences and raising the threshold would make prosecuting these offences more challenging.

9.45 Parliament has determined that if someone suspects that property is criminal property and does one of the prohibited acts to property that is in fact criminal despite the existence of such a suspicion that is sufficient to warrant criminality. For these reasons,

---

[19] *R v Saik* [2006] UKHL 18, [2006] 2 WLR 993.

in the absence of compelling evidence that the test for the offence should be altered, it would not be appropriate to amend it by a sidewind designed to make a change to the reporting regime. We propose to retain the threshold of suspicion for the principal money laundering offences.

9.46 However, as we have acknowledged, the existence of suspicion, which is the threshold for criminality, also serves to prompt the person with that suspicion to make an authorised disclosure. We have already considered at length how the suspicion based trigger for authorised disclosures does not promote the filing of SARs of the best quality and detail.

9.47 In addition, in the context of the threshold for the principal money laundering offences, the impact of an authorised disclosure is intrusive and has a demonstrable impact on the subject of the SAR, whether as an individual or a business. Such a disclosure has financial implications and can cause severe reputational damage.

9.48 Adopting a reasonable grounds to suspect test for the regulated sector in relation to authorised disclosures should, as with required disclosure, promote a more evidence-based approach before DAML SARs are lodged. Once suspicion must be adjudged to be reasonable or based on reasonable grounds, the existence of relevant supporting facts is vital.

9.49 There is also an impact on resources for both the NCA and law enforcement agencies where unnecessary or poor-quality DAML SARs are lodged. A reasonableness requirement would increase the threshold for reporting but without going so far as to require the higher standards of belief or knowledge which would impede the flow of SARs to significantly.[20] By requiring more than merely a subjective suspicion and introducing a more evidence-based approach, it would reduce the number of authorised disclosures without at the lowest end of suspicion or unusual activity. This is an attractive argument given that we have identified in Chapter 1 that there is a high volume of reports, not all of which are useful.

9.50 Requiring a reporter to have reasonable grounds for their suspicion would provide an additional safeguard for those who are the subject of a SAR. Where a suspicious activity report is lodged requesting consent to proceed[21], the delay can be terminal for a business. The impact of freezing an account can be severe and comparable to the immediate consequences to an individual under arrest; it is invasive and prevents a business from acting. It is comparable to a period of 'detention' for a business and can last up to 7 days (excluding the extended moratorium period provided for in the Criminal Finances Act 2017). Given the loss that can be incurred, requiring reasonable grounds to suspect could make the process more proportionate and fair. As George and Brown argued following the *Saik*[22] judgment:

---

[20] Proceeds of Crime Act 2002, ss 330, 331 and 332.

[21] Now referred to as a defence against money laundering ("DAML").

[22] [2006] EWCA Crim 1654; [2007] 1 W.L.R. 303.

To be obliged to report a suspicion, there only has to be a possibility that is more than fanciful, a test which those who suffer because of a SAR will continue to find difficult to challenge.[23]

9.51 It is important to achieve the appropriate balance between these competing interests. and ensure greater efficiency. It would be desirable to maintain suspicion as the threshold for criminality to facilitate the prosecution of those who launder criminal property. Our aim is to produce a regime which:

(1) retains the low level of suspicion of the offences;

(2) promotes the filing of fewer more focussed and valuable SARs;

(3) impacts more proportionately on customers. Ensuring that a DAML SAR is only lodged where necessary;

(4) DAML SARs are evidence-based;

(5) DAML SARs are more likely to demonstrate a greater probability of money laundering occurring; and

(6) DAML SARs will be of greater assistance to law enforcement agencies.

9.52 One method of achieving this would be to retain the threshold for suspicion (of criminal property) in section 340 of the Proceeds of Crime Act, but to amend the legislation so that a specific defence is created to sections 327, 328 and 329 for an individual operating within the regulated sector. If an individual operating in the regulated sector did not have reasonable grounds to suspect that the property was criminal property, they would not commit an offence even though they might have mere suspicion. The existence of this defence for those who regularly encounter criminal property in the course of their business or profession within the regulated sector may secure the benefits outlined above without sacrificing the advantages of a suspicion threshold for general criminality. Such a modification would still alert law enforcement agencies to potential criminal activity at an early stage whilst providing a better balance between the interests of those operating within the regime and those who may be the subject of a disclosure.

9.53 For clarity, we have set out the current thresholds and the effect of our proposed amendments in a series of tables below in relation to the money laundering and disclosure obligations in POCA:

Provisional Proposals on Thresholds **Money Laundering Offences in Part 7 of POCA**		
Provision	**Current threshold**	**Proposed threshold**

[23] G Brown, & T Evans, The impact: the breadth and depth of the anti-money laundering provisions requiring reporting of suspicious activities, Journal of International Banking Law (2008), p 277.

Section 327	Knows or suspects	Unchanged
Section 328	Knows or suspects	Unchanged
Section 329	Knows or suspects	Unchanged

Provisional Proposals on Thresholds **Disclosure Offences in Part 7 of POCA**		
Provision	**Current threshold**	**Proposed threshold**
Section 330	Knows or suspects; or has reasonable grounds for knowing or suspecting	Knows or has reasonable grounds to suspect
Section 331	Knows or suspects; or has reasonable grounds for knowing or suspecting	Knows or has reasonable grounds to suspect
Section 332	Knows or suspects	Knows or has reasonable grounds to suspect

Provisional Proposals on Thresholds **Reporting Obligations in Part 7 of POCA**		
Provision	**Current threshold**	**Proposed threshold**
Required Disclosure Sections 330, 331 and 332	Knows or suspects; or has reasonable grounds for knowing or suspecting	Knows or has reasonable grounds to suspect
Authorised Disclosure	Knows or suspects	Knows or has reasonable grounds to suspect. This will be the effect of the proposed defence under sections 327, 328 and 329

Compliance issues

9.54 We have also considered whether such a change to "reasonable grounds to suspect" for required disclosure and authorised disclosure tests would meet international standards and EU obligations. As we have established in the preceding chapters,

neither FATF nor the Fourth Money Laundering Directive require the threshold for money laundering offences to be set as low as mere suspicion.

9.55 In respect of the threshold for reporting, the reporting requirements under Article 33 of the Fourth Money Laundering Directive require a disclosure where:

> …the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing … All suspicious transactions, including attempted transactions, shall be reported.

9.56 These terms have been replicated in sections 330 and 331 of the Proceeds of Crime Act 2002. The disclosure offences can be committed where there is knowledge, suspicion or reasonable grounds to know or suspect. Article 33 appears to mandate reports where there is a mere suspicion. However, it is not directly effective and requires implementation. It is also important to remember that sections 330 and 331 create criminal liability in addition to imposing reporting obligations and this is an important distinguishing feature of the UK regime.

9.57 Although Canada is not subject to 4AMLD, FATF have conducted an evaluation of the Canadian anti-money laundering and terrorism financing regime. FATF have assessed Canada to be partially compliant with its recommendations on the reporting of suspicious transactions. Whilst the most recent Mutual Evaluation Report ("MER") recognises that the reporting requirement covers several, but not all elements of the reporting requirement, the commentary does not specifically take issue with the threshold of "reasonable grounds to suspect". The particular deficiencies identified in the report do not relate to the use of the term "reasonable grounds to suspect" as the threshold for reporting.[24]

9.58 Whilst we consider that Canada provides a useful precedent in the context of the FATF recommendations, the position is less clear in respect of compliance with the 4AMLD. However, there has been no definitive guidance from the CJEU on this issue as yet. There is also some ancillary support for suspicion requiring grounds or evidence in the language of the 4AMLD.[25] In addition, the 4AMLD talks about alignment with FATF standards where possible. It states:

> Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even at Union level, without taking into account international coordination and cooperation, would have very limited effect. The measures adopted by the Union in that field should therefore be compatible with, and at least as stringent as, other actions undertaken in international fora. Union action should continue to take particular account of the FATF Recommendations and instruments of other international bodies active in the fight against money laundering and terrorist financing. With a view to reinforcing the efficacy of the fight against

---

[24] Recommendation 20 and Financial Action Task Force, Anti-money laundering and counter-terrorist financing measures: Canada Mutual Evaluation Report at http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf (last accessed on 28 May 2018) p 157.

[25] Recital (13) and Article 3(6)(a)(ii) of the Fourth Money Laundering Directive both refer to the presence or absence of "grounds" for suspicion in different contexts.

money laundering and terrorist financing, the relevant Union legal acts should, where appropriate, be aligned with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the 'revised FATF Recommendations').[26]

9.59 If we followed a *Saik*[27] approach to the phrase "reasonable grounds for suspicion", this incorporates a cumulative test of subjective suspicion founded on objective grounds. However, it is unclear what the word "suspicion" adds in Article 33 or indeed sections 330 and 331 of the Proceeds of Crime Act 2002. This has yet to be tested by domestic courts or the CJEU. As we discussed above, the preliminary ruling in *Safe Interenvios, SA v Liberbank, SA*[28], provides support for the view that suspicions must be grounded and cannot be considered a purely subjective matter. If a threshold of "reasonable grounds for suspicion" is not compliant with our EU obligations under 4AMLD, it must be noted that we are in a period of uncertainty as the UK negotiates its exit from the EU. It is unclear to what extent the UK will seek to comply with 4AMLD following Brexit but it is anticipated that compliance with 4AMLD will continue for the foreseeable future.

Statutory guidance on reasonable grounds for suspicion

9.60 The benefits that we have outlined in respect of issuing statutory guidance for required disclosures would also apply if the threshold for authorised disclosures was amended to "reasonable grounds for suspicion". We examined the Canadian model which adopts reasonable grounds to suspect as the threshold for reporting and uses guidance to good effect. The advantages of guidance in line with the Canadian approach can be summarised as follows:

(1) As guidance provides a list of objective factors which may provide reasonable grounds to suspect, it identifies common facts with "predictive capabilities" and highlights irrelevant or unimportant factors which may lead to an unnecessary disclosure;

(2) Money laundering is dynamic and ever-changing. Through guidance, reporters hear directly from law enforcement agencies what types of evidence are indicative of money laundering or terrorist financing. This is an ongoing process and guidance can be adapted as criminals move into different patterns of behaviour or activity. It focuses on risk rather than compliance.

(3) Arguably, reporters, the Financial Intelligence Unit and law enforcement agencies would all be in a better position to evaluate the strength of a suspicion. Disclosures could be triaged and prioritised more quickly if reporters were addressing key indicators in a consistent format. Consistent terminology would feed in to key word searches which are conducted by the FIU and law enforcement agencies to locate relevant material for an investigation.

---

26 Recital (4), Fourth Money Laundering Directive.

27 [2006] UKHL 18; [2007] 1 AC 18.

28 Opinion of Advocate General Sharpston, Case C-235/14 *Safe Interenvios, SA v Liberbank*, SA; Banco de Sabadell, SA and Banco Bilbao Vizcaya Argentaria, SA Official Journal of the European Union, C 235, Vol. 57, 21 July 2014.

9.61 If statutory guidance is drafted to expand on the meaning of reasonable grounds to suspect, its value is likely to be greater if there is input from all of the relevant stakeholders involved in the anti-money laundering regime. Guidance which emanates from discussion between all stakeholders in the process will enable agreement to be reached on what may constitute a ground of suspicion. This is particularly important where there are areas of contention, such as whether it is legitimate to profile customers based on their country of origin. This minimises the risk of reporters applying discriminatory or inappropriate grounds of suspicion. For example, Canada's FINTRAC guidance reminds reporters that "behaviour is suspicious, not people".[29]

9.62 In conclusion, we provisionally propose amending the threshold for required disclosures and authorised disclosures whilst retaining the suspicion threshold for criminality, subject to the defence outlined above. We also invite consultees' views on whether statutory guidance on "reasonable grounds to suspect" would benefit reporters, were the threshold for reporting to be amended.

Consultation Question 6.

9.63 We provisionally propose that the threshold for required disclosures under sections 330, 331 and 332 of the Proceeds of Crime Act 2002 should be amended to require reasonable grounds to suspect that a person is engaged in money laundering. Do consultees agree?

Consultation Question 7.

9.64 If consultees agree that the threshold for required disclosures should be amended to reasonable grounds for suspicion, would statutory guidance be of benefit to reporters in applying this test?

Consultation Question 8.

9.65 We provisionally propose that the suspicion threshold for the money laundering offences in sections 327, 328, 329 and 340 of the Proceeds of Crime Act 2002 should be retained. Do consultees agree?

[29] FINTRAC, Guideline 2 Suspicious Transactions, para 8. http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp#s3-1. Accessed on 28 May 2018.

Consultation Question 9.

9.66 We provisionally propose that it should be a defence to the money laundering offences in sections 327, 328 and 329 if an individual in the regulated sector has no reasonable grounds to suspect that property is criminal property within the meaning of section 340 of the Proceeds of Crime Act 2002. Do consultees agree?

COMMISSION OF INQUIRY INTO STATE CAPTURE

Chapter 10: Criminal property and mixed funds

OVERVIEW

10.1 Once a bank employee becomes suspicious that the bank is holding criminal funds in a customer's account, the employee is at risk of committing one of the three principal money laundering offences by continuing to hold those funds, or dealing with them in one of the ways prohibited under sections 327, 328 or 329 of the Proceeds of Crime Act 2002.

10.2 For example, an individual may receive a monthly salary from their employer and have £1000 of legitimate funds in their bank account. They may make what the bank believes to be a fraudulent loan application and receive a further £3000. The customer may request a withdrawal of £1000. Once the bank suspects that the customer has benefited from a crime, it must seek consent before processing this transaction for the customer.[1] That involves filing a defence against money laundering suspicious activity report ("DAML SAR").

10.3 Because the bank employee suspects criminal conduct, the bank employee also suspects that the bank is holding a mixed fund consisting of legitimate and potentially illicit funds in the customer's bank account. In practice, most of the stakeholders in the banking sector informed us that their practice is to freeze the entire account containing £4000, even though the bank's suspicion relates only to the £3,000 in loaned funds. The bank would then make an authorised disclosure (DAML SAR) to the NCA and seek consent for the £1000 withdrawal to comply with their legal obligations and to obtain a defence against a money laundering charge.

10.4 The practice of freezing entire accounts, regardless of the value of the property that is suspected to be criminal, can have significant economic consequences for a customer. As we discussed in Chapter 2, any customer who is the subject of an authorised disclosure by their bank will be unable to access funds in their bank account during the statutory seven-day notice period whilst the NCA considers the request for consent. Their funds may be frozen for a longer period if their case extends into the moratorium period. After the recent changes in the Criminal Finances Act 2017, there is now the prospect of extending the moratorium period up to a maximum of 186 days. For customers this means that they may not be able to receive any legitimate income such as social security benefits or their salary. Any direct debits or standing orders will also fail during this time. If the customer is a business, it will be unable to receive income or make payments to customers, employees and suppliers. Stopping cash flow for even a short period can be fatal to a small business.

10.5 For larger enterprises, the consequences can be just as profound. In *N v S,*[2] N was a regulated payment services provider. N held approximately 60 active accounts with a large retail bank. These comprised main accounts and separate "client" sub-accounts

---

1 Proceeds of Crime Act 2002, s 340.

2 [2017] EWCA Civ 253, [2017] 1 WLR 3938.

in sterling and various foreign currencies. The main accounts had a high volume of transactions and an annual turnover of around £700 million. A number of clients of N were suspected of fraud. The bank suspected that victims of the fraud had paid money into N's accounts so that they therefore contained criminal property. The bank's response was to freeze the relevant accounts preventing N from executing its clients' instructions. Freezing on this scale meant that individual customers were unable to execute important transactions such as sending funds to complete the purchase of a family home.

10.6 Stakeholders who practise in this area of law and advise customers on these issues were concerned that restricting entire accounts had dire economic consequences for their clients. Moreover, those customers who are the subject of a SAR will not be put on notice due to the tipping off provisions which we outlined in Chapter 2. They are unable to intervene or make representations to the UKFIU or law enforcement agencies. Whilst any application to extend the moratorium period may allow the subject of a SAR to make representations, at that stage it may well be too late.[3]

10.7 A customer may initiate civil proceedings where their account is frozen. Stakeholders in the banking sector and practitioners were concerned by the costs incurred in parallel civil litigation.[4] As it was put in *Squirrell*:

> In the result, if Squirrell is entirely innocent it may suffer severe damage for which it will not be compensated. Further, the blocking of its account is said to have deprived it of the resources with which to pay lawyers to fight on its behalf. Whether or not that is so in this case, it could well be so in other, similar cases. Whatever one might feel were Squirrell guilty of wrongdoing, if, as it says, it is innocent of any wrongdoing, this can be viewed as a grave injustice.[5]

10.8 In addition, this could lead to multiple SARs being lodged where further transactions are undertaken on a "mixed fund".

10.9 One solution to this problem would be for banks to ringfence funds to the value of the suspected criminal property. If the bank were able to preserve a sum equivalent to the value of the funds that are suspected to be criminal rather than restricting the entire account, it may prevent unnecessary economic loss to the customer. Returning to our example above, funds could be preserved in this case by transferring £3000 (the equivalent value of the suspected fraudulent loan money) into another account within

---

3 Extensions up to a maximum of 186 days. See Criminal Finances Act 2017, Pt 1, s 10(2) (s 335(6A) in force, October 31, 2017, subject to transitional provisions specified in SI 2017 No.991 reg 3(1)). See Proceeds of Crime Act 2002, ss 335(6A), 336A, B, C, and D. See Home Office Circular 008/2018 Criminal Finances Act: extending the moratorium period for suspicious activity reports. See Criminal Procedure Rules Part 47.

4 In *Shah v HSBC Private Bank* [2010] EWCA Civ 31, [2010] 3 All ER 477, the customer claimed damages against his bank for failure to comply with his instructions and for other breaches of duty. In *K Ltd v National Westminster Bank plc* [2006] EWCA Civ 1039, [2007] 1 WLR 311, an interim injunction was sought by the customer requiring the bank to comply with instructions. In *Squirrell Ltd v National Westminster Bank plc (Customs and Excise Commissioners intervening)* [2005] 2 All ER 784, [2006] 1 WLR 637 the customer applied for an order that the accounts be unfrozen.

5 *Squirrell Ltd v National Westminster Bank plc (Customs and Excise Commissioners intervening*) [2005] EWHC 664 (Ch) at para [7], [2006] 1 WLR 637.

the bank. This would ensure that the suspected offender could not spend the proceeds of their crime but would allow them access to their legitimate income. However, stakeholders in the banking sector felt that the law was unclear on whether they could treat mixed funds in this way.

Fungibility

10.10 From our pre-consultation discussions with stakeholders in the banking sector, a large number perceive a principal cause of the problem we have explained above to be the principle of fungibility. In short that term is used to describe the fact that, in economic terms, money is considered to be an asset capable of mutual substitution:[6] one £5 note can be substituted for any other £5 note. The funds are "fungible."

10.11 The bank-customer relationship is essentially a debtor-creditor relationship. When a customer deposits money with their bank, the bank is able to treat it as its own. The bank's contractual obligation is to return an equivalent amount to the customer:

> Money, when paid into a bank, ceases altogether to be the money of the principal…it is then the money of the banker, who is bound to return an equivalent by paying a similar sum to that deposited with him when he is asked for it…The money placed in the custody of a banker is, to all intents and purposes, the money of the banker, to do with it as he pleases; he is guilty of no breach of trust in employing it; he is not answerable to the principal if he puts it into jeopardy, if he engages in a hazardous speculation; he is not bound to keep it or deal with it as the property of his principal; but he is, of course, answerable for the amount, because he has contracted, having received that money, to repay to the principal, when demanded, a sum equivalent to that paid into his hands.[7]

10.12 Fungibility creates practical problems for banks when a bank account contains both legitimate income and criminal funds. In the context of our example above, as the criminal funds have now been mixed in with non-criminal funds, the bank cannot isolate or distinguish the £3000 which is suspected to be the proceeds of crime. This problem is compounded when we consider the large number of electronic transactions taking place where there are no physical notes or coins moving into or out of a bank account.

10.13 Some stakeholders felt that the only solution was to freeze the entire account where there was a suspicion that an account contained some criminal property. Other stakeholders took a more pragmatic approach and ringfenced funds by transferring the suspicious amount into another account. However, they lacked confidence that they had legal protection for this course of action.

10.14 The legal position on fungibility in the context of the Proceeds of Crime Act 2002 is uncertain. In 2007, the issue was considered in a Home Office Consultation Paper and the concerns of the British Bankers' Association (now UK Finance) were outlined:

> It is the unified view of the BBA's Money Laundering Advisory Panel that this regime cannot easily be reconciled with the wide definition of criminal property in POCA and the principle of fungibility. It is their view that money in a bank account (as opposed to

---

6 David Fox, *Property Rights in Money* (2008), p 25.

7 *Foley v Hill* (1848) 2 HLC 28, 9 ER 1002, pp 1005 to 1006

notes and coins) is fungible and that as a matter of property law a bank account is a single "indistinguishable mixed fund". Consequently, payments into an account can no longer be distinguished from the wider account. According to this view, once a suspicious transaction has been made, that transaction could be argued to have tainted the rest of the account, and possibly any other account held by the same individual. This would imply that all subsequent transactions on the suspect accounts become acts of money laundering under the provisions of sections 327-29.[8]

10.15 In the same report, the Home Office acknowledged that it was unclear whether the courts would extend the established principle of fungibility into the operation of Part 7 of the Proceeds of Crime Act 2002 and the anti-money laundering regime. Even if fungibility did apply to the operation of Part 7, an alternative analysis is available. If, as in our example above, £3000 of criminal money is paid into a bank account with a credit of £1000, it is arguable that this will become mixed with the bank's money and legal title to 'the money' as a whole will pass to the bank. The customer does not have a specific £1000 in the bank, in legal terms he or she has a "chose in action" (also known as a "thing in action") to the value of the money deposited. That is simply a right to sue the bank for that sum of money. The "thing in action" represents the criminal property, not the funds in the account. On one analysis, the bank has provided consideration for the money deposited. That consideration is in the form of the "thing in action", and so possession of the mixed funds will not be an offence under section 329 of the Proceeds of Crime Act 2002. As a result, the whole account will not be tainted. It is unclear whether a bank is protected from an offence under section 328 of the Proceeds of Crime Act 2002 on this analysis. That is because the offence under section 328 is broader and encompasses arrangements which facilitate the acquisition, retention use or control of criminal property. However, the bank would still be able to protect against criminal liability by making an authorised disclosure (DAML SAR). The exemption under section 328(2) of the Proceeds of Crime Act 2002 would then apply.

10.16 The "thing in action" analysis accords with the approach the courts have taken to the interpretation of the Proceeds of Crime Act 2002 confiscation regime. For the purposes of confiscation proceedings at the end of a criminal case, the court will not necessarily recover the original property that was generated by criminal activity. Instead, the court will make a finding as to the value of an offender's benefit and will then seek repayment of that debt from an offender's remaining assets. Whilst it is imperative that a bank preserves funds to the value of the suspected criminal property, under the Proceeds of Crime Act 2002, a bank is not expected to trace and retain the physical notes and coins that it originated from. That would be impossible in an electronic transfer of funds.

10.17 However similar problems also arise from the definition of criminal property in section 340 of the Proceeds of Crime Act 2002 and its impact on mixed funds. We turn now to consider the issue of mixed funds generally and whether the current law in Part 7 meets the challenges presented by modern banking practices.

Mixed funds

10.18 The decision of the Court of Appeal in *Causey* provides the basis for the proposition that once criminal funds and legitimate funds are mixed, the whole amount becomes

---

[8] Home Office, *The Consent Regime 2007 and Fungibility*, para 4.9.

criminal property.[9] In that case it was alleged that the offender had transferred money into the account of a third party in order to evade confiscation proceedings. The prosecution argued that the money in the account was the direct proceeds of crime from a conspiracy to steal and to handle motor vehicles and "car ringing".[10]

10.19 The Court considered the question of what constituted the "proceeds of criminal conduct" (or "benefit from criminal conduct" as it would now be considered under the Proceeds of Crime Act 2002).[11] The Court held that the expression "proceeds of criminal conduct" was broad, and even without the addition in the section of the words "in whole or in part, directly or indirectly", it appeared to cover any property or financial advantage even if it was only partly obtained in connection with the criminal conduct. Therefore, if money was obtained partly in connection with the commission of an offence and partly in some other connection, it would be treated as obtained in connection with the offence. The prosecution submitted (and the Court accepted) that "if one penny or penny's worth of the property dealt with is the proceeds of criminal conduct then the section is satisfied.[12]

10.20 In *N v RBS*,[13] the bank argued, and the Court of Appeal accepted, that because "criminal property" is defined very broadly under section 340 of the Proceeds of Crime Act 2002, "the result is that if only a small part of the property can be traced to crime, *all of it* constitutes criminal property" (emphasis added). The Court agreed citing *R v Causey*.[14]

10.21 There appear to be two lines of reasoning behind the Courts' expansive interpretation. The first, is the definition of "criminal property" and the interpretation of "in whole or in part".[15] As we outlined in Chapter 2, property is caught by the provisions in Part 7 of the Proceeds of Crime Act 2002 where it constitutes a person's benefit from criminal conduct or it represents such a benefit ("in whole or part and whether directly or indirectly"). Thus, in *William and others*,[16] the Court of Appeal (Criminal Division) cited the definition of "property" in section 340(3) of the Proceeds of Crime Act 2002, and stated:

> The reference to "in whole or in part" is important because it shows that the whole property is treated as criminal property, even where only part of it represents benefit from criminal conduct.

---

9 *R v Causey*, Court of Appeal (Criminal Division); unreported, 18 October 1999. The court was interpreting Criminal Justice Act 1988, s 93C which has the same definition of criminal property as the Proceeds of Crime Act 2002, s 340.

10 *R v Causey*, Court of Appeal (Criminal Division); unreported, 18 October 1999, p 2.

11 Criminal Justice Act 1988, s 102(1).

12 Criminal Justice Act 1988, s 93C(1): "property which is, or in whole or in part directly or indirectly represents, the defendant's proceeds of criminal conduct."

13 [2017] EWCA Civ 253, [2017] 1 WLR 3938, at [80].

14 *R v Causey*, Court of Appeal (Criminal Division); unreported, 18 October 1999.

15 Proceeds of Crime Act 2002, s 340(3).

16 [2013] EWCA Crim 1262, [2015] Lloyd's Rep FC 704.

10.22 The second line of reasoning is the definition of "benefit" in section 340 of the Proceeds of Crime Act 2002. A person benefits from conduct if he or she obtains property as a result of *or in connection with* the conduct. Focussing on this wording, the reasoning appears to be that property that is obtained "*both*" in connection with "criminal conduct" and some other connection must mean that the "other" is a reference to legitimate property.

10.23 If *Causey* accurately represents the law, then a bank is prevented from transferring or making payments from an account in respect of which legitimate money and criminal property have been "mixed" because, to do that would constitute an offence contrary to section 327 of the Proceeds of Crime Act 2002.[17] This has the practical effect of preventing a bank from ringfencing funds whilst awaiting a decision on consent having served a DAML SAR. If a bank could identify that only part of the account resulted from criminal activity, it would be more proportionate to allow the account to be operated as long as the value of the criminal funds was preserved.

10.24 In *Squirrell*[18] Her Majesty's Customs and Excise ("HMCE") argued that the bank had no option but to freeze the entire account where part was suspected to be criminal.[19] This submission appeared to be adopted by the Court. However, the Court also observed that the obligation on the bank was not to move *suspect funds or property* for the duration of the notice period and possibly the moratorium period.[20] It appears to have been assumed that the only means by which funds could be preserved was to block the entire account.

10.25 However, there is also some support in the case law for mixed funds being separable and capable of being distinguished. In *R v Smallman and another,*[21] gambling winnings were mixed with "criminal property" obtained by fraud. The Court of Appeal remarked that it did not follow that because MS was in profit as a gambler that the transfers he made to AS did not consist of or represent the proceeds of the fraud "in whole or in part" and that "it was open to the jury to conclude that the money transferred represented, in part at least, MS's benefit from criminal conduct. The Court did not approach the issue on the basis that the entire mixed fund constituted "criminal property".[22]

10.26 The Court of Appeal in *Moran*[23] considered section 102(5) of the Criminal Justice Act 1988, an interpretation clause similar to section 340 of the Proceeds of Crime Act 2002:

---

17 Or indeed Proceeds of Crime Act, ss 328 and 329.

18 *Squirrell Ltd v National Westminster Bank plc (Customs and Excise Commissioners intervening)* [2005] ECHC 664 (Ch), [2005] 2 All ER 784.

19 *Squirrell Ltd v National Westminster Bank plc (Customs and Excise Commissioners intervening*) [2005] ECHC 664 (Ch), [2005] 2 All ER 784, para 6.

20 *Squirrell Ltd v National Westminster Bank plc (Customs and Excise Commissioners intervening)* [2005] ECHC 664 (Ch), [2005] 2 All ER 784 at para 18.

21 [2010] EWCA Crim 548.

22 Proceeds of Crime Act 2002, s 340(3); para 174.

23 [2001] EWCA Crim 1770; [2002] 1 WLR 253.

> References in this Part of this Act to property obtained, or to a pecuniary advantage derived, in connection with the commission of an offence include a reference to property obtained or to a pecuniary advantage derived, both in that connection and in some other connection.

10.27 The Court in *Moran*[24] expressed the view that it appeared that Parliament was contemplating a benefit or pecuniary advantage stemming from connected activities, as for example where an offender committed a criminal offence and sold his story to a newspaper.

10.28 In the Northern Irish case of *R v Ho Ling Mo*,[25] the appellant was a solicitor convicted of fraud and on two counts of removing criminal property contrary to section 327(1)(e) of the Proceeds of Crime Act 2002. Funds obtained as a result of fraudulent legal aid claims were placed into accounts and then apparently transmitted to China. The prosecution case was that once a person knew or suspected that fraudulently obtained money had been placed into an account, thereby increasing the balance of the account owing to the account holder, "the chose in action which is the entitlement of the account holder to the balance from the bank becomes criminal property."[26] It was not argued on appeal that this analysis was incorrect. The Court of Appeal for Northern Ireland held that the "concession that the lodgement of fraudulently obtained monies into a bank account thereby increasing the balance owing to the account holder constitutes criminal property is clearly properly made". The Court, in *Ho Ling Mo*, observed that its reasoning accorded with *R v Causey* when interpreting similar provisions in the Criminal Justice Act 1988.[27]

Other approaches in the Proceeds of Crime Act 2002

Mixed property in civil recovery

10.29 In cases where lawfully acquired property has been mixed with criminally acquired proceeds, Parliament and the courts have taken a different approach to determining the value of "recoverable property" for the purposes of civil recovery.[28]

10.30 Where legitimate money and criminal funds have been mixed, only that amount which relates to unlawful conduct can be recovered. This is referred to in the Proceeds of Crime Act 2002 as "mixed property". For example, an offender may purchase a house with tainted and untainted funds; if half of the price comes from tainted money, only half of the value of the property is to be regarded as derived from crime.[29]

10.31 This approach to mixed funds broadly aligns with equitable principles of tracing where an individual may trace his or her money into another person's bank account. Where a trustee mixes trust money with money in his or her own bank account, the money in that

---

24 [2001] EWCA Crim 1770; [2002] 1 WLR 253.

25 [2013] NICA 49.

26 [2013] NICA 49 at p 24.

27 See also *R v Ramsey* [2016] NICA 13, where *Causey* is cited in the judgment.

28 Proceeds of Crime Act 2002, s 306.

29 *Director of the Assets Recovery Agency v Olupitan* [2008] EWCA Civ 104; [2008] CP Rep 24.

account belongs to the trustee and the beneficiaries in the amounts that they originally provided.[30]

Restraint orders and confiscation

10.32 A restraint order prevents criminal assets from being dissipated by an offender whilst he is awaiting trial. The purpose of seeking a restraint order is to preserve assets at an early stage with a view to any subsequent application for confiscation at the conclusion of the criminal case.[31] As we discussed in the preceding chapters, one of the objectives of the consent regime is to pause transactions whilst law enforcement agencies decide if they wish to take action to restrain assets. When a bank restricts or blocks an account, it is able to preserve funds which law enforcement agencies may seek to restrain.

10.33 It is important to note at this point that if a court proceeds to a confiscation hearing at a later date, they will have to consider whether the offender has a "criminal lifestyle".[32] If so, the court can assume that property coming into the offender's hands over the preceding six years is as a result of his or her criminal conduct.[33] This broadens the scope of an offender's benefit considerably. If the offender does not have a criminal lifestyle, then the court will consider whether he or she benefited from their particular criminal conduct.

10.34 The confiscation process will place a value on an offender's benefit. Once the value of any benefit has been identified, the court will determine what the offender's available assets are. The available assets will then be applied to satisfy the debt.

10.35 In the making of a restraint order, where the amount of an offender's benefit can be identified, Millington and Sutherland Williams argue that the prosecutor should not seek to restrain assets significantly in excess of that figure.[34] However, there will be difficulty in some cases in identifying, at the restraint stage, exactly what the offender's benefit is said to be. There may be grounds to restrain all of an offender's assets where they may have a criminal lifestyle for the purposes of confiscation proceedings.[35]

A way forward on the issue of mixed funds

10.36 During our pre-consultation discussions, stakeholders in the banking sector understandably sought greater clarity on this issue. Law enforcement stakeholders agreed that there was little value in a SAR that was reporting an internal transaction made to preserve funds. Ringfencing criminal funds would also provide a sensible and practical solution to the risks of economic loss and hardship to those who are the subject of a SAR. The issue of mixed funds requires a practical and proportionate approach. It is strongly arguable that there should be a consistent approach in principle across the

---

30 David Fox, Property Rights in Money (2008), para 7.56.

31 Proceeds of Crime Act 2002, s 40(1).

32 Proceeds of Crime Act 2002, s 75(1).

33 Proceeds of Crime Act 2002, s 10.

34 *Millington and Sutherland Williams on the Proceeds of Crime* (2018) at 2.42.

35 Proceeds of Crime Act, 2002, s 75 and Schedule 2. See also *Re K* [2005] EWCA Crim 619, [2006] BCC 362.

Proceeds of Crime Act 2002 and that principles of civil recovery offer the most fair and proportionate solution.

10.37 It is our provisional proposal that where the value of the suspected criminal property is clear and readily ascertainable, banks should be permitted to ringfence funds to that amount without having to seek consent. We have proposed one method of ringfencing based on our pre-consultation discussions with stakeholders. However, we welcome consultees' views on whether there are other ways of preserving suspected criminal property such as restricting a bank account to prevent the balance from falling below an amount equal to the suspected criminal property.

10.38 Our provisional view is that the obligation to make a required disclosure[36] should remain. The submission of a SAR may still provide useful intelligence to law enforcement agencies but we welcome consultees' views on this.

10.39 We provisionally propose amending the offences in sections 327, 328 and 329 to provide that no criminal offence is committed by an individual where:

(1) they are an employee of a credit institution;

(2) they suspect [*or if our earlier proposal in Chapter 9 is accepted* have reasonable grounds to suspect] that funds in their possession constitute a person's benefit from criminal conduct;

(3) the suspicion [*or if our earlier proposal in Chapter 9 is accepted* reasonable grounds to suspect] relates only to a portion of the funds in their possession;

(4) the funds which they suspect [*or if our earlier proposal in Chapter 9 is accepted* have reasonable grounds to suspect] constitute a person's benefit from criminal conduct are either:

(a) transferred to an account within the same credit institution; or

(b) the balance is not allowed to fall below the level of the suspected funds;

(5) they conduct the transaction in the course of business in the regulated sector (as defined in Schedule 9 of the Proceeds of Crime Act 2002); and

(6) the transfer is done with the intention of preserving criminal property.

10.40 Amending the offences would provide protection for banks who exercised their discretion and adopted a pragmatic approach. It would be limited in scope and we believe would have a positive impact by reducing the number of DAML SARs resulting from these types of transaction.

10.41 We have considered whether the definition of criminal property in section 340(3) of the Proceeds of Crime Act 2002 ought to be amended. We acknowledge that the current definition may be problematic. However, we believe that the terms of reference for our review are too narrow in scope to consider such a change. There are wider issues

[36] Proceeds of Crime Act 2002, ss 330, 331 and 332.

relating to how we identify criminal property for the purposes of the Proceeds of Crime Act 2002 as a whole. Any amendment to the definition may impact on related parts of the Proceeds of Crime Act 2002, such as restraint and confiscation. We observe that the Law Commission has agreed with the Home Office to review the law on confiscation in Part 2 of the Proceeds of Crime Act 2002 in 2018. It may be appropriate to include this issue within that review to ensure that a consistent approach is taken throughout the Proceeds of Crime Act 2002.

Consultation Question 10.

10.42 Does our summary of the problems presented by mixed funds accord with consultees' experience of how the law operates in practice?

Consultation Question 11.

10.43 We provisionally propose that sections 327, 328 and 329 of POCA should be amended to provide that no criminal offence is committed by a person where:

(1) they are an employee of a credit institution;

(2) they suspect [*or if our earlier proposal in Chapter 9 is accepted have reasonable grounds to suspect*] that funds in their possession constitute a person's benefit from criminal conduct;

(3) the suspicion [*or if our earlier proposal in Chapter 9 is accepted reasonable grounds to suspect*] relates only to a portion of the funds in their possession;

(4) the funds which they suspect [*or if our earlier proposal in Chapter 9 is accepted have reasonable grounds to suspect*] constitute a person's benefit from criminal conduct are either:

(a) transferred to an account within the same credit institution; or

(b) the balance is not allowed to fall below the level of the suspected funds;

(5) they conduct the transaction in the course of business in the regulated sector (as defined in Schedule 9 of the Proceeds of Crime Act 2002); and

(6) the transfer is done with the intention of preserving criminal property.

10.44 Do consultees agree?

COMMISSION OF INQUIRY INTO STATE CAPTURE

COMMISSION OF INQUIRY
INTO STATE CAPTURE

Chapter 11: The scope of reporting

11.1 The combined effect of a low reporting threshold (suspicion), an "all crimes" approach and a broad definition of criminal property is to capture a wide range of activity which banks and businesses are required to report on pain of criminal sanction.[1] We have engaged in pre-consultation discussions with a large number of stakeholders who have direct reporting responsibilities or represent those who do, across a broad range of sectors. In addition, we have had pre-consultation discussions with law enforcement agencies and in particular, the National Crime Agency ("NCA"). The majority of those stakeholders have identified situations generating Suspicious Activity Reports ("SARs") which are taking valuable resources to investigate but there is little intelligence value to be gleaned from them. There is no means of "switching off" the reporting obligation even where both the reporter and the NCA know it is unlikely to be useful.

11.2 Given this broad consensus, we have sought to identify ways to avoid these SARs being made.

11.3 Stakeholders with reporting obligations told us that there was a gap between the legislative provisions and industry guidance on what may constitute a "reasonable excuse" for failing to make a disclosure. This lack of definitive guidance on the interpretation of the legislation makes it very difficult for reporters to act with confidence, even where it is clear that the intelligence value of a SAR will be low. This was widely believed to lead to defensive reporting.

11.4 It is our provisional view that statutory guidance should be issued which would catalogue examples of situations in which there would be a reasonable excuse not to make a required[2] and/or an authorised disclosure,[3] depending on the nature of the SAR, its potential value to law enforcement agencies and whether any transaction ought to be stopped pending investigation. The guidance would assist reporters by giving examples of these circumstances.

11.5 We considered the merit of making proposals for legislative change to provide for specific exemptions to address individual types of SAR but have discounted that approach. In order to provide legal certainty, a legislative amendment defining "reasonable excuse" in Part 7 of the Proceeds of Crime Act 2002 ("POCA") would need to take the form of an exhaustive list of the types of SARs which are considered to be of little value.[4] This list would, of course, be liable to change. Capturing these SARs in legislation risks inhibiting valuable flexibility in the way the NCA can make the system work in response to changes in money laundering behaviour and other legislation which may impact on SARs. Whilst we recognise that statutory guidance is not ideal, setting

---

1 At present, reporters will only avoid criminal liability if they fall within one of the specified exemptions to the principal money laundering offences or the disclosure offences.

2 Proceeds of Crime Act 2002, ss 330, 331, and 332.

3 Proceeds of Crime Act 2002, ss 327(2)(b), 328(2)(b), 329(2)(b) and 328.

4 Or for the list to be capable being amended frequently and easily.

out examples of circumstances in which that a reporter may have a reasonable excuse not to report seems to us to be a better solution than legislative amendment.

11.6 Guidance is more easily updated, and would provide useful flexibility, allowing the system to adapt to changes in money laundering behaviour and the needs of law enforcement agencies. Potential unintended consequences could be monitored on an ongoing basis, and the guidance amended accordingly. The regime could be more responsive, and this should reduce or stop the flow of those types of SARs which have been identified by the NCA as of limited value.

Consultation Question 12.

11.7 We provisionally propose that statutory guidance should be issued to provide examples of circumstances which may amount to a reasonable excuse not to make a required and/or an authorised disclosures under Part 7 of the Proceeds of Crime Act 2002. Do consultees agree?

11.8 The following paragraphs examine the types of disclosures that stakeholders have told us are of little value or utility to law enforcement agencies and how they might be addressed in statutory guidance. We note that this is a non-exhaustive list and we welcome evidence from consultees on any other types of disclosure that might be included.

Low value transactions

11.9 Money laundering can be committed in relation to criminal property to the value of 1p, £1 or £1 million. There is no provision to exclude low value transactions from the obligation to report. One of the main objectives in reporting suspicious activity is to allow law enforcement agencies time to seize or seek to restrain criminal assets. Low value transactions are unlikely to be pursued for two reasons. First, provisions for the seizure and forfeiture of cash do not authorise seizure for amounts of less than £1000.[5] Secondly, deploying the resources of law enforcement agencies to recover a small sum would be disproportionate and therefore unlikely to occur in practice.

11.10 Some stakeholders have argued that a de minimis threshold should be introduced below which no reporting obligations should apply. Depending on the level at which this threshold was set, this has the potential to reduce the volume of required and authorised disclosures filed without damaging the overall intelligence value of the system.

11.11 As we outlined in Chapter 2, the legislation provides that banks ("deposit taking bodies") who suspect criminal property is represented in an account have a limited exemption if they continue to make transactions provided the sums involved are under the threshold amount (currently set at £250). This permits small payments for living expenses or cash

[5] Proceeds of Crime Act 2002, s 294(3). Proceeds of Crime Act 2002 (Recovery of Cash in Summary Proceedings: Minimum Amount) SI 2006 No 1699, para 2.

withdrawals to be made.[6] A higher threshold can be requested and authorised.[7] However, other businesses in the regulated sector do not benefit from this exemption and will have to make an authorised disclosure regardless of the value of the criminal property involved in the transaction. Nonetheless, as noted above, the threshold is low and may not reflect the average level of current payments to meet living expenses in the real world.

11.12 A de minimis threshold applying across the regulated sector would mean that no offence would be committed where the value of the criminal property is below the threshold. This would avoid the administrative burden of making an authorised disclosure in low value transactions and seeking consent in each case.

11.13 One of the main disadvantages of introducing a general de minimis threshold is the risk that offenders would adapt their behaviour in line with any published threshold to avoid detection. It is clear that money launderers can be sophisticated in their avoidance techniques. For example, under the present law "structuring" or "smurfing" is the practice of executing financial transactions in a pattern to avoid financial thresholds.

11.14 There is no doubt that in some situations a low value transaction can provide useful intelligence, or arise in a circumstance where it would generally be desirable for a disclosure to be made. For example, if a vulnerable person was being defrauded of a relatively small sum, a disclosure to the NCA would bring this to the attention of law enforcement agencies and provide the opportunity to intervene. However, this may result in duplication of reporting where the reporter suspects a low value fraud has been committed which we will discuss below.

11.15 Moreover, as "smurfing" shows, repeated small value transactions attract attention as being unusual and indicative of money laundering. Reports that reflect that may have an intelligence value.

11.16 An exemption for low value transactions may also conflict with our obligations under Article 33 of the Fourth Money Laundering Directive ("4AMLD") which requires that:

> Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly: (a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases…

11.17 As we have previously indicated, although the impact of Brexit is unclear at the time of writing, we foresee that the UK will continue to comply with the terms of 4AMLD. Notwithstanding whether our obligations under 4AMLD would allow for such a change, taking into account that a limited exemption already exists for banks, the most important justification for continuing to report low value transactions is to ensure vital intelligence is not lost for law enforcement agencies in terrorism investigations. As we discussed in Chapter 3, it is increasingly common for terrorism to be funded by low level criminal

---

6 Proceeds of Crime Act 2002, ss 327(2C), 328(5), 329(2C) and 339A.

7 Proceeds of Crime Act 2002, s 339A(3)(b).

activity and small amounts of money. If a minimum financial threshold for reporting were to be introduced, this may disproportionately affect the flow of intelligence in relation to suspected terrorism.

11.18 We have considered and concluded that introducing a minimum financial threshold for money laundering but not for terrorism financing would be unworkable. At a minimum, it would present administrative challenges for reporters. Of greater concern is that terrorism may be financed by ordinary criminal activity. Reporters may not appreciate that there is any link to terrorism. Intelligence related to terrorism financing may be picked up from a required or an authorised disclosure which the reporter did not associate with terrorism in any way.

11.19 It is our provisional view that there should not be a minimum financial threshold for required or authorised disclosures. However, we invite consultees to give their views on this issue and any evidence on the practical impact of reporting low-value transactions. Likewise, we would welcome consultees' views on the operation of the current threshold amount in light of current levels of payments to meet living expenses. We invite consultees' views on whether the current threshold amount which applies to banks should be raised above £250.

Consultation Question 13.

11.20 It is our provisional view that introducing a minimum financial threshold for required and authorised disclosures would be undesirable. Do consultees agree?

Consultation Question 14.

11.21 Do consultees believe that the threshold amount in section 339A of the Proceeds of Crime Act 2002 should be raised? If so, what is the appropriate threshold amount?

Internal movement of funds

11.22 As we discussed in Chapter 10, a bank may need to move funds internally with the aim of preserving them and preventing an offender from dissipating them. Under the current law, this requires the submission of an authorised disclosure and the grant of appropriate consent. Subject to acceptance of our proposal in Chapter 10 which would render the following otiose, it is our provisional view that authorised disclosures of this nature are of little value to law enforcement agencies. Statutory guidance could confirm that an internal transfer for the purpose of preserving criminal property would amount to a reasonable excuse for not making an authorised disclosure.

Consultation Question 15.

11.23 We provisionally propose that any statutory guidance issued should indicate that the moving criminal funds internally within a bank or business with the intention of preserving them may amount to a reasonable excuse for not making an authorised disclosure within the meaning of sections 327(2)(b), 328(2)(b) and 329(2)(b) of the Proceeds of Crime Act 2002.

11.24 Do consultees agree?

Duplicate reporting obligations

11.25 Reporters may have obligations, over and above those in POCA, to report the same information to more than one body. One example of this is suspected fraudulent transactions. One large reporting bank estimated that 80% of their DAML SARs related to fraud. Further to making either a required or authorised disclosure, a report would be made to Action Fraud, which is the reporting mechanism for the National Fraud Intelligence Bureau within the City of London Police. The information is provided directly to law enforcement agencies via this route. This means that time is expended on two reports; one goes directly to law enforcement agencies, the other via the NCA. Stakeholders have identified this duplication as a problem and some were unclear about to which bodies they should report.[8]

11.26 As we discussed in the preceding Chapters, not all reports to law enforcement agencies provide the same opportunities to intervene in criminal activity. An authorised disclosure provides law enforcement agencies with the opportunity to disrupt criminal activity at an early stage. An authorised disclosure also prevents a transaction relating to property suspected to be criminal from continuing. There may be some circumstances in which an authorised disclosure would be the preferred mechanism for notifying law enforcement agencies as to fraud.

11.27 We provisionally propose that statutory guidance should be provided on appropriate reporting routes to minimise duplication where possible. The following provisional proposals are predicated on the existence of such guidance to enable reporters to lodge reports which are of the most value to law enforcement agencies with the correct law enforcement agency. We invite consultees to provide evidence of duplicate reporting obligations.

[8] Home Office and HM Treasury, Joint Action Plan for anti-money laundering and counter-terrorist finance (April 2016), p 40.

Consultation Question 16.

11.28 Do consultees agree that there is insufficient value in required or authorised disclosures to justify duplicate reporting where a report has already been made to another law enforcement agency (in accordance with the proposed guidance)?

11.29 Further, we propose that in accordance with guidance, lodging a report with another law enforcement agencies agency should amount to a reasonable excuse not to make a required disclosure.

Consultation Question 17.

11.30 We provisionally propose that statutory guidance be issued indicating that a failure to make a required disclosure where a report has been made directly to a law enforcement agency on the same facts (in accordance with proposed guidance on reporting routes) may provide the reporter with a reasonable excuse within the meaning of sections 330(6)(a), 331(6) and 332(6) of the Proceeds of Crime Act 2002. Do consultees agree?

Information in the public domain

11.31 Some stakeholders reported instances of having made disclosures where the information amounting to the suspicion about the property was already in the public domain. For example, where a property transaction by a high net worth individual is widely reported in the media. In these cases, where the disclosure provides no more information than is already in the public domain, it may be of little value to law enforcement agencies.

11.32 Arguably, in such cases there should be no obligation on the reporter to make a disclosure. However, there are at least two issues that arise in creating such an exception:

(1) How can a reporter be confident that the information is "in the public domain? What types of source of publication would be sufficient?

(2) Would it be sufficient that the information existed on one source or should multiple sources be required?

11.33 Some sources may be deemed to be less reliable than others. It would be difficult to define with any confidence a comprehensive list of those sources which a reporter must have consulted before being considered to have a reasonable excuse for not making a disclosure. For example, blogs or informal sources of information may be considered to be less reliable than mainstream news outlets, but may host considerable information.

11.34 Such an exception would be difficult to apply where a reporter was in possession of more facts than those reported by the media, possibly from multiple sources. This would

pose difficulties in discerning whether the level of information known to the reporter was equivalent to that which was already in the public domain. This may also require the analysis of multiple sources to identify any differences.

11.35 A further difficulty with a public information exception is that it would place an additional burden on law enforcement agencies to monitor information that is in the public domain. Given the volume of media reports and the frequency with which new reports are disseminated, it may not be appropriate to remove the obligation to disclose from those who are party to a transaction and place it on law enforcement agencies.

11.36 It is our provisional view that disclosures should continue to be made, even where some or all of the information may be in the public domain. However, the burden of this may be mitigated by requiring a short-form report in which any relevant media source could be identified. This short-form report could be prescribed under section 339 of POCA.

Consultation Question 18.

11.37 We provisionally propose that a short-form report should be prescribed, in accordance with section 339 of the Proceeds of Crime Act 2002, for disclosures where information is already in the public domain. Do consultees agree?

Property transactions within the UK

11.38 As we have discussed in Chapters 2 and 4, one of the main objectives of the consent regime is to enable law enforcement agencies to investigate and restrain funds within the statutory timescales. Where criminal funds are to be invested in property or applied to mortgage payments and are not leaving the UK, there is an audit trail leading to an identifiable asset. Arguably urgent action is unnecessary in these circumstances as the money is applied to immoveable property, although the intelligence relating to the transaction may well be of value to law enforcement agencies.

11.39 From our pre-consultation discussions with stakeholders, whilst law enforcement agencies will benefit from the intelligence provided in an authorised disclosure in such a situation, no immediate action is likely to be taken by investigators. This means that consent will usually be granted for such transactions. Authorised disclosures will nevertheless impose an additional burden on resources.

11.40 We provisionally propose that an authorised disclosure should not be required where the transaction relates to property within the UK. We further propose that continuing with a transaction, without making an authorised disclosure, where suspicious funds are being applied to or invested in property in the UK should amount to a reasonable excuse for the purposes of the money laundering offences. Transactions would therefore continue without the need for consent but reporters would still be obliged to make a required disclosure. Intelligence would still be fed into law enforcement agencies but without preventing the transaction from taking place.

Consultation Question 19.

11.41 We provisionally propose that statutory guidance should be issued indicating that it may amount to a reasonable excuse to a money laundering offence not to make an authorised disclosure under sections 327(2), 328(2) and 329(2) of the Proceeds of Crime Act 2002 where funds are used to purchase a property or make mortgage payments on a property within the UK. Do consultees agree?

Consultation Question 20.

11.42 We provisionally propose that the obligation to make a required disclosure in accordance with sections 330, 331 and 332 of the Proceeds of Crime Act 2002 in these circumstances should remain? Do consultees agree?

Multiple transactions and related accounts

11.43 Where an account contains criminal funds and multiple transactions or payments are due to be made, under the current law an authorised disclosure would need to be made seeking consent for each transaction. Further, where an individual or company has more than one account, a series of inter-linked transactions would result in multiple disclosures. This imposes an unnecessary administrative burden on the reporter. It also leads to multiple related reports which might better be incorporated into one composite document.

11.44 We provisionally propose that reporters should be permitted to lodge one report which provides a reasonable description of the activity on the account. Likewise, if a person has more than one account, there should be flexibility in the reporting system to allow for one complete report to be filed rather than separate and broadly similar reports. This would be subject to safeguards outlined in guidance to ensure the appropriate level of detail was provided where a single report was submitted dealing with multiple transactions.

Consultation Question 21.

11.45 We provisionally propose that reporters should be able to submit one SAR for:

(1) multiple transactions on the same account as long as a reasonable description of suspicious activity is provided; and/or

(2) multiple transactions for the same company or individual.

11.46 Do consultees agree?

Repayment to victims of fraud

11.47 A bank may identify that a fraud has been committed by monitoring customer transactions. Under the current law, where they detect fraud, they will need to lodge a DAML SAR seeking consent to pay funds back to the victim. Although the funds technically constitute criminal property, they belong to the victim who has been defrauded. Generally, in such cases reporters will also have made a duplicate report to Action Fraud.

11.48 We provisionally propose that a bank should not have to seek consent to repay a victim of fraud where the bank has already lodged an appropriate report with Action Fraud.

Consultation Question 22.

11.49 Do consultees agree that banks should not have to seek consent to pay funds back to a victim of fraud where they have filed an appropriate report to Action Fraud?

Historical crime

11.50 Some stakeholders, particularly in the legal sector, were concerned that they may have to make a disclosure where they uncovered minor criminal offences which were committed many years ago, such as failing to obtain software licences. In such cases, it was difficult to identify the criminal property or fully ascertain the facts. A disproportionate amount of time might be spent on investigation before a disclosure could be made. The disclosure itself may be of little value as a result.

11.51 It is unclear whether there is value in receiving disclosures that relate to historical crime. If they are of little utility to law enforcement agencies and are disproportionately costly to prepare, statutory guidance on reasonable excuse might address the best approach to reducing the regulatory burden created by the obligation to make disclosures in relation to historical crime.

Consultation Question 23.

11.52 Do consultees believe that there is value in disclosing historical crime?

Consultation Question 24.

11.53 How long after the commission of a criminal offence would a disclosure be considered historical for the purposes of law enforcement agencies?

No UK nexus

11.54 During pre-consultation discussions with stakeholders, we were told that disclosures may be made to the NCA where there is no UK nexus. For example, in a global

organisation, the investigative team and any nominated officer may be based in the UK. However, the transaction they are reviewing might have no connection to the UK. In these circumstances, it may be that the transaction should be reported to a Financial Intelligence Unit in another jurisdiction.

11.55 It is our provisional proposal that, where the transaction has no UK nexus, it should amount to a reasonable excuse not to make a required or authorised disclosure. Statutory guidance could assist by ensuring that reports are made to the appropriate Financial Intelligence Unit.

Consultation Question 25.

11.56 We provisionally propose that statutory guidance be issued indicating that where a transaction has no UK nexus, this may amount to a reasonable excuse not to make a required or authorised disclosure. Do consultees agree?

Disclosures instigated by law enforcement agencies

11.57 Stakeholders reported to us that they felt it was unclear whether there was value in making a disclosure where their suspicion arose solely from enquiries made by law enforcement agencies. If our provisional proposals in Chapter 9 are accepted, statutory guidance cataloguing factors which may found a suspicion would resolve this issue. An enquiry from a law enforcement officer, without more, would not amount to reasonable grounds to suspect that another person was engaged in money laundering. Nor would it found a suspicion that property was criminal property without the existence of some additional ground.

Other types of disclosure

11.58 As we outlined at the beginning of this Chapter, we are aware that this list is non-exhaustive. Consultees may have identified other types of SAR that are of little effect or value to law enforcement agencies. We welcome further evidence from consultees on types of disclosure which are required under the current law but do not provide valuable and/or actionable intelligence.

Consultation Question 26.

11.59 Are there are any additional types of SAR under POCA which are considered to be of little value or utility that we have not included?

COMMISSION OF INQUIRY INTO STATE CAPTURE

COMMISSION OF INQUIRY
INTO STATE CAPTURE

Chapter 12: The meaning of consent

12.1 As we discussed in Chapter 2, the concept of "appropriate consent" is fundamental to the authorised disclosure exemption under section 338 of the Proceeds of Crime Act 2002 ("POCA"). Seeking appropriate consent is the mechanism by which the authorised disclosure exemption operates. A person does not commit one of the three principal money laundering offences if:

> he makes an authorised disclosure under section 338 and if the disclosure is made before he does the act mentioned in subsection (1), he has the appropriate consent.[1]

12.2 "Appropriate consent" is defined in section 335 of POCA. The appropriate consent (for the purposes of the authorised disclosure exemption) is:

> the consent of a nominated officer (constable/customs officer) to do a prohibited act if an authorised disclosure is made…

12.3 A similar exemption exists, under section 21ZA of the Terrorism Act 2000, although the legislation employs the term "arrangements with prior consent".

> A person does not commit an offence under any of sections 15 to 18 by involvement in a transaction or an arrangement relating to money or other property if, before becoming involved, the person—
>
> (a) discloses to an authorised officer the person's suspicion or belief that the money or other property is terrorist property and the information on which the suspicion or belief is based, and
>
> (b) has the authorised officer's consent to becoming involved in the transaction or arrangement.[2]

12.4 The majority of stakeholders that we spoke to during our pre-consultation discussions questioned whether the word "consent" in Part 7 of POCA was the most appropriate term to describe the formal process that now operates in this context. In this chapter, we will consider whether there are alternatives which would improve, or more accurately describe, that process.

12.5 In order to analyse whether the term "consent" is the most suitable, it is important to understand the objectives behind the consent process. The seeking and granting of consent has a practical function: when an individual makes an authorised disclosure setting out their knowledge or suspicion of criminal property, any financial transaction is paused whilst the UK Financial Intelligence Unit ("UKFIU") within the National Crime Agency ("NCA") considers whether consent should be granted. This process is intended to protect those who will inevitably encounter suspected criminal property in the course of business or in a professional capacity. No criminal offence is committed by the

---

[1] Proceeds of Crime Act 2002, ss 327(2)(a), 328(2)(a) and 329(2)(a).

[2] Terrorism Act 2000, s 21ZA(1).

reporter where an authorised disclosure is made and consent to proceed with an act otherwise proscribed by sections 327-329 of POCA is given.

12.6 The consent process brings important intelligence regarding criminal activity to the attention of law enforcement agencies. Consent requests may provide the NCA and law enforcement agencies with opportunities to disrupt criminal activity or restrain or recover assets. The seven-day period[3] for which the bank must pause the transaction provides law enforcement agencies with the time to investigate.[4]

Problems with the term "consent"

12.7 The ordinary meaning of consent is to give permission for something to happen or to agree to it.[5] It is not clear that that meaning accurately describes the interaction between the reporting body and the UKFIU where an authorised disclosure is made under Part 7 of POCA. On a natural understanding of the concept, a grant of consent conveys the impression that the UKFIU approves of the transaction or has sanctioned it. It may also indirectly signify that the transaction has been cleansed of any criminality, not just in relation to the conduct of the reporter for the principal money laundering offences. That may lead to the impression that the property in question is no longer criminal which is not strictly the case.

12.8 The limitations of consent were considered in *AP, U Limited v CPS, RCPO*[6], where the Court stated that:

> Consent may relieve the bank of any criminal responsibility for a transaction in question; but that does not mean that in relation to others involved in the transaction, it may not amount to or form part of a dishonest money laundering scheme.[7]

12.9 What "appropriate consent" provides might be more accurately described as some limited 'exemption' for the reporting body in relation to a specific transaction.

12.10 Aside from its failure to describe accurately the legal consequences of the action of reporting, there is some evidence that the term consent lacks clarity and is misunderstood. In July 2016, the UKFIU reviewed its operating procedures around consent. It found that the term "consent" was frequently misinterpreted, with the consequence that reporters might be seeking consent inappropriately. For example, a bank might ask a customer to provide personal information to verify his or her identity. If the customer failed to respond, the bank would be unable to complete its due diligence checks on the customer. In the circumstances, there may be insufficient information on which to form a suspicion, but in some such cases reporters might make an authorised disclosure seeking consent to proceed with a transaction. It would be of little intelligence

---

3 Proceeds of Crime Act 2002, s 335(5).

4 And any subsequent moratorium period, Proceeds of Crime Act 2002, ss 335(6) and 336A.

5 https://en.oxforddictionaries.com/definition/consent (last accessed on 22 May 2018), https://www.collinsdictionary.com/dictionary/english/consent (last accessed on 22 May 2018) https://dictionary.cambridge.org/dictionary/english/consent (last accessed on 22 May 2018).

6 [2007] EWCA Crim 3128, [2008] 1 Cr App R 39.

7 [2007] EWCA Crim 3128, [2008] 1 Cr App R 39 at 511.

value. In other circumstances the ambiguity of the term had led to reporters erroneously withdrawing a consent request during the notice period, or failing to provide a key piece of information.[8]

12.11 Approximately 3326 consent SARs between October 2015 and March 2017 were affected by these issues. This represents a significant proportion of the total number of SARs seeking consent where money laundering was suspected over the same period (27,471). [9] Disclosures under the Terrorism Act do not appear to trigger the same issues. It is of note that the number of terrorism related disclosures is much lower when compared with money laundering (422 terrorism financing disclosures seeking consent compared to 27,471 money laundering disclosures seeking consent).[10]

Current approach

12.12 Following its review, the UKFIU chose to adopt new terminology to describe the process. It adopted the terms "defence against money laundering" ("DAML") and "defence against terrorism financing" ("DATF") as replacement terms for "appropriate consent" and "arrangements with prior consent". The UKFIU believes that this terminology more accurately reflects the intention behind the legislative provisions and will improve the quality of authorised disclosures whilst reducing unnecessary requests.[11] In recent guidance, the NCA stated:

> A DAML does not differ legally from the 'consent' that was previously notified, other than in the wording; the meanings are one and the same. The term 'consent' previously gave rise to misinterpretation and confusion among some reporters in terms of its legal effect – for instance some interpreted (incorrectly) that the NCA was providing clearance or tacit permission to reporters, when in fact the legal effect is (and always was) solely a defence to a money laundering offence under POCA.[12]

12.13 In addition, when appropriate consent is granted, the UKFIU now issues written clarification as to the effect of such a grant. It informs reporters that the grant of consent only provides a defence to one of the three principal money laundering offences under sections 327-329 of the Proceeds of Crime Act 2002. Granting a request does not:

(1) cleanse the property or the transaction;

(2) absolve individuals from their professional conduct duties or any regulatory requirements;

(3) provide individuals with a defence from other criminal or regulatory offences;

---

8 National Crime Agency, *Suspicious Activity Reports Annual Report 2017*, p 17-20.

9 National Crime Agency, *Suspicious Activity Reports Annual Report 2017*, p 20.

10 National Crime Agency, Suspicious Activity Reports Annual Report 2017, p 6.

11 National Crime Agency, *Suspicious Activity Reports Annual Report 2017*, p 18.

12 National Crime Agency, SARs regime good practice frequently asked questions defence against money laundering (May 2018). http://www.nationalcrimeagency.gov.uk/publications/902-defence-against-money-laundering-faq-may-2018/file p 3 (last accessed on 26 May 2018).

(4) oblige the reporter to proceed with the transaction; nor

(5) override the private law rights of any person who may be entitled to the property.[13]

12.14 During our pre-consultation discussions with stakeholders, there was some support for this recent change in terminology. However, some also suggested that the change may have created a new source of confusion. Abandoning the statutory language of appropriate consent without any legislative amendment or statutory guidance could, it is argued, create uncertainty for those with disclosure and reporting obligations. What is more, some stakeholders believed that the adoption of an entirely different term, other than consent or DAML, might be more appropriate.

Alternative terms

12.15 We have examined a number of alternative terms that were suggested by stakeholders during pre-consultation discussions.

12.16 The term "immunity" was raised as one possibility. Some stakeholders argued that "immunity" was preferable because it conveyed more accurately what is being sought by the bank and offered by the NCA: protection from prosecution where an authorised disclosure has been made. However, given the breadth of this term it may present similar problems in operation to "consent". In other words, it could convey to a reporter an inappropriate level of certainty that his or her subsequent actions would not constitute a criminal offence and that no prosecution could result from them.

12.17 Some stakeholders suggested that the term "waiver" would be a more appropriate substitute for "consent". "Waiver" is a term employed in, for example, legal professional privilege and contract law. It does import a concept of permissiveness. It could indicate that law enforcement agencies authorities were waiving their right to pursue a prosecution for one of the principal money laundering offences on the basis that an authorised disclosure had been made. However, its origins lie in civil rather than criminal law, where, for example, the law recognises that someone may forego strict contractual rights or accept incomplete or deficient performance of a contract. It does not seem accurate to describe the NCA as having a "right" to prosecute.

12.18 A further alternative might be to describe the interaction as one seeking an exemption from criminal liability for the offences. As we discussed in Chapter 2, the wording of sections 327(2), 328(2) and 329(2) state that a person does not commit an offence if he makes an authorised disclosure under section 338 of the Proceeds of Crime Act. We explained why these sections might be more appropriately referred to as an exemption rather than a defence. This provides scope for adapting the terminology to "an exemption from a criminal offence under section 327, 328 or 329 of the Proceeds of Crime Act 2002." The difficulty with this approach is that the essence of the exemption is permission to perform an otherwise prohibited act. Any amendment would not change the nature and quality of the legal act of granting consent.

---

[13] See also National Crime Agency, SARs regime good practice frequently asked questions defence against money laundering (May 2018). http://www.nationalcrimeagency.gov.uk/publications/902-defence-against-money-laundering-faq-may-2018/file p 5 (last accessed on 26 May 2018).

12.19 For the same reasons, we have considered and discounted the term "permission". Whilst it is synonymous with the term consent and therefore describes the process behind the exemption, amending the legislation in this way would amount to a superficial change and would confer no real benefit.

12.20 In summary, we see no significant benefit to any of the alternative terms suggested. What is more, employing any of the alternative terms would not change the way the law operates. Any change in terminology would be merely presentational and intended to improve understanding of the current law.

Options for reform

12.21 After considering the range of alternative terms that may be used to describe the process of seeking and securing "appropriate consent", we have also considered the implications of changing the language of the statute without making any substantive changes to the legal effect or meaning of the sections. There are several points to note.

12.22 First, there is a presumption that legislation must effect a change in law. *Craies on Legislation* notes:

> In approaching statutory construction the courts will generally assume that every word used by the legislature is intended to have some legislative effect.[14]

12.23 As we have described, legislation designed to alter the terminology but not the legal effect of the provision would fall foul of this principle. It would not make any substantive change to the law or alter the nature of the exemption. Arguably substituting a different term would not be intended to have any legislative effect.

12.24 The Office of Parliamentary Counsel define good law as law that is "necessary, clear, coherent, effective and accessible."[15] Merely substituting another term for "appropriate consent" may be desirable but it is difficult to argue that it is necessary. For this reason, whilst there are other terms which could be used to substitute "consent", we do not propose that the term should be changed in the legislation.

12.25 In Chapter 9, we provisionally proposed that statutory guidance should be issued on the term suspicion. We observed that statutory guidance may have a positive impact on reporting by reducing unnecessary reports. Similar considerations apply in relation to the term "appropriate consent". If our objective is to improve understanding of the current law rather than changing it, guidance would provide the most suitable means of achieving this. Statutory guidance which addressed the issues noted above could provide greater clarity and certainty for reporters. We have considered the existing NCA guidance on appropriate consent. We note that its focus is on good practice in the submission of a suspicious activity report rather than giving formal guidance on the current law. There are strong arguments in favour of providing one source of formal guidance from Government issued under a statutory power on appropriate consent within the meaning of sections 327(2)(a), 328(2)(a) and 329(2)(a), 338 of the Proceeds of Crime Act 2002.

---

14 Daniel Greenberg, *Craies on Legislation* (9th Ed, 2008) at 20.1.23.

15 https://www.gov.uk/guidance/good-law#good-law-the-challenge (last accessed 8 June 2018)

12.26 We provisionally propose that statutory guidance on the process of making an authorised disclosure would be beneficial.

12.27 We do not make any such proposal in respect of "arrangements with prior consent" under the Terrorism Act 2000. As noted above the volume of disclosures is much lower than in the context of money laundering. Further, the available evidence suggests that the current terrorism financing regime is working effectively. However, we invite consultees' views on whether this accords with their experience in practice and whether guidance on "arrangements with prior consent" would be beneficial.

Consultation Question 27.

12.28 We provisionally propose that there should be a requirement in POCA that Government produces guidance on the concept of "appropriate consent" under Part 7 of the Act. Do consultees agree?

Consultation Question 28.

12.29 Based on their experience, do consultees believe that statutory guidance on arrangements with prior consent within the meaning of section 21ZA of the Terrorism Act 2000 would be beneficial?

COMMISSION OF INQUIRY INTO STATE CAPTURE

Chapter 13: Information sharing

THE NEED FOR EFFECTIVE INFORMATION SHARING

13.1 The Financial Action Task Force ("FATF") has highlighted the importance of effective information sharing to a well-functioning anti-money laundering and counter-terrorism financing regime.[1] As we discussed in Chapter 2, currently there are two ways in which information can be shared between banks and law enforcement agencies, otherwise than through the required and authorised disclosure mechanisms.[2] First, information can be channelled through the Joint Money Laundering Intelligence Taskforce ("JMLIT") relying on a statutory gateway which facilitates this exchange.[3] Secondly, the Criminal Finances Act 2017 made provision for voluntary bank-to-bank sharing (in conjunction with the National Crime Agency ("NCA") of information in connection with a suspicion to enable one "Super-SAR" to be lodged.[4] It is hoped that combining information in this way will lead to a better understanding of relevant intelligence for law enforcement agencies.

13.2 Our pre-consultation discussion with stakeholders revealed two ways in which the current position could be improved. First, existing powers allow for voluntary information sharing in connection with a suspicion within the regulated sector.[5] There is no legal provision which allows for information sharing within the regulated sector where a suspicion has not yet been formed, for example where a bank employee detects unusual activity on an account which does not trigger a suspicion within the meaning assigned to that term by the courts. This can impact on reporting in two ways; the absence of the further information which would trigger a suspicion may mean that no disclosure is made. Useful intelligence may be lost. However, if a concern cannot be allayed by seeking further information, risk-averse reporters may be more likely to make a disclosure which has minimal intelligence value given the risk of criminal liability for failing to do so. Secondly, some stakeholders argued that there would be merit in broadening the membership of the JMLIT.

13.3 Before considering these suggestions in more detail, we first briefly set out the relevant legal background.

Existing provisions to obtain and share information

13.4 As we have seen, there are existing channels for obtaining and sharing information, albeit not at the pre-suspicion stage. They provide a route for obtaining intelligence from multiple sources within the regulated sector. As we discussed in Chapter 2, the JMLIT

---

1 Financial Action Task Force, "*Public Consultation on the Draft Guidance for Private Sector Information Sharing",* p 3.

2 Proceeds of Crime Act 2002, ss 327(2), 328(2), 329(2), 330 to 332 and 338.

3 Crime and Courts Act 2013, s 7.

4 Proceeds of Crime Act 2002, ss 339ZB to ZG. These provisions are only partially in force. See Chapter 2.

5 Proceeds of Crime Act 2002, ss 339ZB to ZG. These provisions are only partially in force. See Chapter 2.

Taskforce has already achieved significant success through information sharing. Between May 2016 and March 2017, JMLIT reported instigating more than 1000 bank led investigations into customers suspected of money laundering; the identification of more than 2000 accounts previously unknown to law enforcement agencies and the restraint of £7m of suspected criminal funds.[6]

13.5 This partnership between law enforcement agencies and the financial sector functions under the existing gateway in section 7 of the Crime and Courts Act 2013. This broad provision allows any person to disclose information to the NCA if the disclosure is made for the purposes of the exercise of any NCA function.

13.6 At the centre of this taskforce, is an Operations Group which includes officers from the NCA, Her Majesty's Revenue and Customs ("HMRC"), City of London Police, Metropolitan Police Service, the Serious Fraud Office ("SFO"), the Financial Conduct Authority ("FCA"), Cifas[7] and vetted staff from thirteen banks. Investigators attend this group to brief members on their investigations and make requests for information. One of the stated purposes of the JMLIT Operations Group is to assist banks and law enforcement agencies through data sharing where suspected money laundering crosses multiple financial institutions. One of the advantages of data sharing in this forum is the ability to prioritise and speed up enquiries by having access to a large number of banks at the same time.[8]

13.7 In addition to the voluntary information sharing provisions which are only partially in force at the time of writing and are as yet untested, Further Information Orders ("FIOs"), were introduced by the Criminal Finances Act 2017.

13.8 The NCA may make an application to the magistrates' court for a FIO. Further information can be sought from a bank or business which submitted a SAR or another bank or business in the regulated sector. The court will make a FIO where it is satisfied that the information would assist:

(1) in investigating whether a person is engaged in money laundering; or

(2) in determining whether an investigation of that kind should be started; and

(3) it is reasonable in all the circumstances for the information to be provided.[9]

13.9 Failure to comply with a further information order can result in a financial penalty.[10] As the order is not limited to the bank or business which made the disclosure, this may

---

6 http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit (last accessed on 21 May 2018).

7 Cifas is a not-for-profit fraud prevention membership organisation in the UK. See https://www.cifas.org.uk/about-cifas/what-is-cifas (last accessed 17 July 2018).

8 http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit (last accessed on 21 May 2018) and www.nationalcrimeagency.gov.uk/publications/808-jmlit-toolkit-june-2017 pp 4 to 6, (last accessed on 21 May 2018).

9 Proceeds of Crime Act, s 339ZH.

10 Proceeds of Crime Act, s 339ZH(8).

provide a useful tool and contribute to a broader understanding of the intelligence context. It also safeguards the customer's interests by providing for NCA involvement imposing a reasonableness test and appropriate judicial oversight at the application stage.

13.10 Furthermore, law enforcement agencies have a number of additional powers at their disposal to obtain further information on individuals such as Production Orders,[11] Customer Information Orders,[12] Account Monitoring Orders,[13] and Disclosure Orders.[14] The precise requirements for obtaining such orders vary depending on the specific conditions and the nature of the investigation, but broadly there must be reasonable grounds to suspect that the person specified in the order has committed a money laundering offence.[15]

13.11 These methods of obtaining information provide two safeguards for the individual who is the subject of such an investigation. First, reasonable grounds to suspect that a person has committed a money laundering offence are required. Secondly, there is judicial oversight and scrutiny of the grounds for such an application.

Data protection provisions

13.12 Information sharing within the anti-money laundering community must be considered within the context of the UK's obligations under the existing data protection regime. This is primarily found in the EU's General Data Protection Regulation ("GDPR"), and the UK's Data Protection Act 2018, the relevant provisions of which we briefly describe below.

The General Data Protection Regulation

13.13 The GDPR came into force on 25 May 2018. It is directly effective. Article 5 of the GDPR requires that personal data shall be:

(1) processed lawfully, fairly and in a transparent manner in relation to individuals;

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

---

11 Proceeds of Crime Act 2002, s 345(1).

12 Proceeds of Crime Act 2002, s 363.

13 Proceeds of Crime Act 2002, s 370.

14 Proceeds of Crime Act 2002, s 357(2).

15 Proceeds of Crime Act 2002, ss 346 (Production Orders), 365(4) (Customer Information Orders), 371(4) (Account Monitoring Orders) and 358 (Disclosure Orders).

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed are erased or rectified without delay;

(5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

(6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

13.14 For banks or businesses, the lawful basis for processing data is the legal obligation imposed by Part 7 of the Proceeds of Crime Act 2002 to process personal data in order submit a SAR to the NCA when they know or suspect that a person is engaged in, or attempting, money laundering.[16]

13.15 Article 10 of the GDPR mandates that personal data relating to criminal convictions and offences should be processed under the control of official authority unless specifically authorised with appropriate safeguards.[17]

13.16 Article 23 of the GDPR allows Member States to introduce exemptions. Specific provision is made for the purposes of safeguarding the prevention, investigation, detection or prosecution of criminal offences. Any restriction must be necessary and proportionate and respect the essence of the individual's fundamental rights and freedoms.[18]

The Data Protection Act 2018

13.17 The Data Protection Act 2018 received Royal Assent on 23 May 2018. It repeals the Data Protection Act 1998, replaces the existing law and supplements the provisions of the GDPR.

13.18 The Data Protection Act 2018 makes specific provision for data processing in the context of law enforcement. In Part 3 of the Act, there are six data protection principles

---

16 Article 6(1) (c) of the General Data Protection Regulations (EU) 2016/679: "processing is necessary for compliance with a legal obligation to which the controller is subject." Proceeds of Crime Act 2002, ss 330, 331 and 332 provide the legal obligation to disclose.

17 Article 10 of the General Data Protection Regulations (EU) 2016/679. Schedule 1, Part 1 of Data Protection Act 2018.

18 Article 23 of the General Data Protection Regulations (EU) 2016/679. See also Information Commissioner's Office Guide to the General Data Protection Regulation (2018) p 176. https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf (last accessed on 12 June 2018).

in relation processing data for law enforcement purposes. These principles are summarised below:

(1) The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair. The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either (a) the data subject has given consent to the processing for that purpose, or (b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.[19]

(2) The second data protection principle is that (a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.[20]

(3) The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.[21]

(4) The fourth data protection principle is that (a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and (b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.[22]

(5) The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.[23]

(6) The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.[24]

13.19 Where data is processed for a law enforcement purpose, the Act provides that the rights of the data subject as set out in sections 44 to 48 of the Act[25] do not apply in relation to the processing of relevant personal data in the course of a criminal investigation or criminal proceedings, including proceedings for the purpose of executing a criminal

---

19 Data Protection Act 2018, s 35.

20 Data Protection Act 2018, s 36.

21 Data Protection Act 2018, s 37.

22 Data Protection Act 2018, s 38.

23 Data Protection Act 2018, s 39.

24 Data Protection Act 2018, s 40.

25 Data Protection Act 2018, Pt 3, ch 3 (ss 43 to 24).

penalty.[26] It also allows for the rights of the data subject to be restricted, in whole or in part, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences. Any restriction must be necessary and proportionate.[27]

13.20 Schedule 2 provides for exemptions from specified obligations under the GDPR. The pre-existing law enforcement agencies exemption in section 29 of the Data Protection Act 1998 was repealed on the 25 May 2018, and has been replaced (in effect) by paragraph 2 of schedule 2 to the Data Protection Act 2018. This provides for an exemption for the purposes of the prevention and detection of crime and the apprehension or prosecution of offenders.

REFORM OPTIONS

Stakeholders' views

13.21 Pre-consultation discussions with stakeholders revealed a range of views, and a number of possible options for reform.

13.22 Some stakeholders suggested that information sharing before the threshold of "suspicion" has been reached might allow the reporter to form a more evidence based suspicion or quickly allay concerns as the case may be. It could also allow for a more pro-active approach to detecting financial crime and increase the quality of intelligence provided to law enforcement agencies. It was noted, however, that sharing information at this stage would require additional legal protection or "safe harbour" to avoid breaching the 2018 Act. Those stakeholders in favour of wider information sharing provisions noted that this protection should extend to any breach of confidence or other data protection laws where information was shared in good faith to prevent and detect economic crime.

13.23 Other stakeholders were unconcerned by this issue, believing that there was unlikely to be any real appetite to share information in this way. They also noted that it could be commercially disadvantageous to pursue this route due to the additional delay incurred. There was also a risk of "contagion": routine enquiries could create suspicion where there were otherwise no real grounds. This could have a negative impact on customers who may find themselves unable to access banking services.

13.24 Some stakeholders also expressed concerns about the voluntary information sharing provisions inserted by the Criminal Finances Act 2017. It was suggested that they were not sufficiently clear to be used by banks and businesses. The provisions are untested and the majority of stakeholders indicated that there was no real incentive to use them. It would always be easier for a bank to submit its own SAR rather than take the additional steps required, incurring further delay. Stakeholders also noted that, having expended more time on a request to share data, it could still be rejected. This concern might be met if information sharing intended to assist in forming or allaying a suspicion was permitted.

13.25 Although existing data protection legislation allows for the sharing of information for the prevention and detection of crime, regulated companies are concerned that there

---

[26] Data Protection Act 2018, s 43(3).

[27] Data Protection Act 2018, ss 44(4)(b), 45(4)(b), 48(3)(b), and 68(7)(b).

should be express legal cover that is directly related to the anti-money laundering regime, in order to reduce the risk of civil litigation for breach of confidentiality. Current guidance from the Home Office includes the caveat that regulated sector institutions using these provisions must consider their obligations under the GDPR separately. This remains an area of uncertainty at the time of writing.[28]

13.26 As we discussed in Chapter 2, JMLIT has proved to be a successful partnership between the financial sector and law enforcement agencies. However, some stakeholders felt disenfranchised by their exclusion from it. Many felt that they could provide more useful intelligence if the membership of JMLIT were expanded or if there was greater dissemination of information, particularly regarding emerging trends in money laundering activity.

Pre-suspicion data sharing

Benefits

13.27 As we discussed in Chapter 2, a bank may detect unusual activity on an account when monitoring transactions using computer algorithms. Any alert will then be investigated and further due diligence checks may be required such as requesting further information from the customer. In some circumstances, it may benefit the customer for the bank to consult another bank to obtain further information. If that information demonstrated that the activity was not suspicious, a disclosure would not need to be made to the NCA and the customer's account would not be restricted. The converse is true; without the information, a bank may make a disclosure to the NCA even though the suspicion is at a very low level and based on limited information.

13.28 Pre-suspicion information sharing may also increase the amount of intelligence that is provided to law enforcement agencies. If one bank identifies activity of concern, another bank may be able to provide additional essential information which assists law enforcement agencies in their understanding and interpretation of relevant intelligence. When these pieces of information are put together, the combined value to law enforcement agencies may be much greater. If this is done at an early stage, i.e. before a suspicion has been formed, this may assist in the prevention and detection of economic crime.

The risk of "debanking" and financial disenfranchisement

13.29 When a bank employee forms a suspicion that there is criminal property in a customer account, he or she will need to comply with the reporting obligations. Additionally, they may make a commercial decision to terminate the bank's contractual relationship with the customer due to the risk that they present. This is commonly described as "de-risking" or "de-banking":

> 'De-risking' or 'de-banking,' refers to the practice of financial institutions exiting relationships with and closing the accounts of clients perceived to be "high risk." Rather than manage these risky clients, financial institutions opt to end the

[28] Home Office Circular: Criminal Finances Act 2017 – Money Laundering: Sharing of Information within the Regulated Sector Sections 339ZB-339ZG, paras 35 to 36.

relationship altogether, consequently minimizing their own risk exposure while leaving clients bank-less.[29]

13.30 Maxwell and Artingstall have observed that the private sector acting alone has relatively little scope to disrupt criminal activity beyond reporting any suspicion. Bringing the customer relationship to an end is the likely consequence where the customer presents a risk. [30] A bank is contractually entitled to terminate its provision of banking services and is entitled to choose its own customers. However, banks have been criticised for terminating customer relationships without a reasonable basis for doing so. It has been estimated that there are approximately 2.5 billion "unbanked" individuals worldwide who lack access to a bank account. "Debanking" can also affect entire communities.

13.31 In May 2013, Barclays opted to partially withdraw from providing banking services to the money service business sector, who provide money remittance and bureaux de change services. Dahabshiil, a money service business registered in England and Wales, which operated in the Horn of Africa, challenged the termination of its contractual relationship with Barclays. [31] This formal legal challenge highlighted the importance of Dahabshiil and money services businesses in general to economies without formal banking structures. Such businesses may provide the only means of transferring money to individuals in countries such as Somalia. Therefore, debanking at this level can lead to the financial exclusion of vulnerable communities:

> Financial institutions have responded by significantly scaling back risk appetites, which has resulted in the wholesale de-banking of entire customer bases.[32]

13.32 Terminating contractual relationships with customers can lead to individuals re-entering the financial system at a weaker point, for example where anti-money laundering or counter-terrorist financing checks are less rigorous. It may also force individuals outside the financial system altogether. For those who are not involved in criminal activity, lack of access to a bank account may lead to financial exclusion. This can be severely disempowering for an individual, restricting their capacity to, for example, rent a home or buy property. For those involved in criminal activity, financial exclusion affects the police's ability to monitor suspect transactions and develop intelligence to assist with any investigation. For example, under section 370 of the Proceeds of Crime Act 2002, an appropriate officer can apply to a Crown Court judge for an Account Monitoring Order. If granted, this order imposes a duty on the bank to provide information on the account for a period of up to 90 days from the date on which the order was made if the conditions are satisfied.[33]

---

29 Tracy Durner, and Liat Shetret, Understanding bank de-risking and its effects on financial inclusion: an exploratory study, *Global Center on Cooperative Security* (2015), p 3. https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/rr-bank-de-risking-181115-en_0.pdf last accessed on 12 June 2018.

30 Nick Maxwell and David Artingstall, Royal United Service Institute for Defence and Security Studies (RUSI), The Role of Financial Information-Sharing Partnerships in the Disruption of Crime (October 2017) p 1.

31 *Dahabshiil Transfer Services Ltd v Barclays Bank Plc* [2013] EWHC 3379 (Ch); [2014] UK CLR. 215.

32 Tracy Durner, and Liat Shetret, Understanding bank de-risking and its effects on financial inclusion: an exploratory study, *Global Center on Cooperative Security* (2015), p 8.

33 Proceeds of Crime Act 2002, s 370.

13.33 In practical terms, bank-to-bank sharing of information about specific customers and their concerns before any suspicion had been formed may only serve to exacerbate existing problems with debanking. Some stakeholders described how concerns about customers could easily become "contagious" between banks without any firm foundation. This might increase the number of commercial relationships which are terminated where the individual is considered a risk by one or more financial institutions rather than actively suspicious. This may be particularly so in terrorism-related cases where there may be little commercial motivation to retain the customer.

13.34 Stakeholders in the NTFIU told us that in cases where there are concerns relating to terrorist financing or other activity, the amounts involved may be comparatively small. Consequently, the customer may only have a small amount of money in their bank account or they might be in debt. They may present as an undesirable customer from a commercial perspective. As such, even low-level concerns may lead to the termination of the banking relationship before any suspicion is formed. In turn, this may frustrate efforts to investigate as the opportunity to gather evidence may be lost.

Data protection considerations

13.35 There are risks to the customer whenever the bank shares their information. As we have discussed, the existing threshold of subjective suspicion is already low. Facilitating the exchange of information before any suspicion had been formed would allow banks to share sensitive and personal customer data where no single individual at the bank actually suspected the customer to be engaged in money laundering.

13.36 As we discussed above, sharing information must take into account obligations to protect personal data. Until recently, this was provided for under the Data Protection Act 1998. This Act gave individuals rights in relation to their personal information and places corresponding obligations on organisations with responsibilities for processing personal data. It was based on eight principles of good data handling.[34] For banks and businesses, the processing of data about their customers and clients may lead to a suspicion that a person is engaged in money laundering. In turn, this may trigger an obligation to disclose personal information about the customer to the NCA.[35]

13.37 However, whilst there is a statutory duty to disclose backed by criminal sanction, the bank or business is also at risk of a request by the customer to see information held about them. Such information may include the fact that a disclosure has been made to the NCA or other sensitive details about that disclosure. Section 29 of the Data Protection Act 1998 provided some protection for the bank or business where personal data was used for purposes connected to crime.[36] As discussed above, this protection has been replicated in the Data Protection Act 2018.

---

[34] Information Commissioner's Office, *Using the crime and taxation exemptions* (s29) (2015), p 2. https://ico.org.uk/media/1594/section-29.pdf accessed on 20 May 2018. Information Commissioner's Office, Data Sharing Code of Practice (May 2011), Annex 1 https://ico.org.uk/media/1068/data_sharing_code_of_practice.pdf (last accessed on 20 May 2018).

[35] Proceeds of Crime Act, ss 330, 331 and 332.

[36] The exemptions also apply to taxation but this is not relevant for the purposes of this Paper.

13.38 Section 29 provided an exemption for banks from the usual data protection principles where specific criteria were met. It had a dual function. First, it allowed a bank to withhold information that should usually be provided to a customer. Secondly, it allowed banks to disclose personal data in ways that would otherwise breach the data protection principles. For example, a bank which disclosed a suspicion that a person was engaged in money laundering (a "required disclosure"[37]) received protection under the Act in two ways:

(1) the Act allowed the bank to disclose the personal data to the NCA without applying the usual data protection principles if the disclosure is necessary for the prevention and detection of crime (or the apprehension or prosecution of offenders)[38];

(2) the bank did not have to fulfil its obligation to tell its customer how their data is being processed or respond to a customer's request for access to their data[39] if doing so would prejudice the prevention or detection of crime. The prejudice must have been real, actual and of substance.[40] Telling a customer how their information had been used or giving them access to the bank's notes about a customer could risk "tipping off" an offender as we discussed in Chapter 2. It could also reveal investigative methods which could be damaging to preventing and detecting crime in the future.

13.39 The exemption under section 29 was fact sensitive. The bank decided on a case by case basis whether the exemption applied in the circumstances.[41] Invoking the section 29 exemption required a significant likelihood of prejudice in the particular case in which it arises.[42] It required the bank to undertake a balancing exercise, taking into account the degree of interference with the customer's fundamental rights that would occur and deciding whether derogating from their obligations would be proportionate.[43] There is nothing to indicate that the constraints on disclosure have been relaxed under the Data Protection Act 2018 and it is likely the case law will continue to apply.

Formulating a pre-suspicion information sharing threshold

13.40 The current wording of the information sharing provisions allows for the sharing of information "in connection with a suspicion". We have looked at three alternative formulations which articulate a pre-suspicion threshold for the sharing of information between banks:

---

37 Proceeds of Crime Act 2002, ss 330 and 331.

38 Data Protection Act 1998, s 29(3).

39 Data Protection Act 1998, s 7.

40 Information Commissioner's Office, Using the crime and taxation exemptions (s 29) (2015), p 5. https://ico.org.uk/media/1594/section-29.pdf (last accessed on 20 May 2018).

41 *R (on the application of Alan Lord) v secretary of State for the Home* Department [2003] EWHC 2073 (Admin).

42 *Zaw Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 QB para 84 and *R (on the application of Alan Lord) v secretary of State for the Home Department* [2003] EWHC 2073 (Admin), [2004] Prison L.R. 65.

43 *Zaw Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 QB, para 76 to 80.

(1) allowing information to be shared for the purposes of determining whether there is a suspicion that a person is engaged in money laundering;

(2) allowing information to be shared for the purpose of preventing and detecting economic crime; or

(3) allowing information to be shared in order to determine whether a disclosure under sections 330 or 331 of the Proceeds of Crime Act 2002 would be required.

13.41 There are some difficulties with these suggested formulations. There remains a tension between pre-suspicion information sharing and data protection provisions. As we discussed earlier, in relation to the previous exemption under section 29 of the Data Protection Act 1998, there was a requirement to demonstrate a significant likelihood of prejudice. It would be very difficult to demonstrate a significant chance of prejudice to the prevention or detection of crime if there was no actual suspicion that the customer was engaged in money laundering.[44]

13.42 In addition, the disclosure obligations in Part 7 of the Proceeds of Crime Act 2002 do not require the bank to act on anything other than information within its possession in deciding whether they are suspicious that a person is engaged in money laundering. There is no obligation in the existing provisions to seek out further information. It cannot be said that sections 330 and 331 make it necessary to exchange information in order to comply with their legal obligations. A bank would be entitled not to make a disclosure if the information in their possession did not go beyond mere cause for concern.[45]

Conclusion

13.43 As we discussed earlier in this paper, there is a strong case for requiring the reporter to have reasonable grounds to suspect before a disclosure is made. There are legitimate concerns that those who are the subject of disclosures are protected by an evidence-based approach to reporting. Given these earlier arguments, there remain significant concerns about allowing private sector institutions to share information below the suspicion threshold and therefore outside the SARs regime. While some stakeholders believe that such a change may improve the efficiency of the reporting regime, it is difficult to quantify this with any certainty.

13.44 Importantly, there are inherent dangers in creating a lower threshold for the sharing of information between non-government actors where commercial interests intersect with legal obligations. There are also strong arguments against allowing private sector institutions to operate at a lower threshold than law enforcement agencies for the obtaining and onward disclosure of information without external scrutiny. Consequently, there is a case for arguing that information sharing where no suspicion about the property has been formed may be inappropriate as a matter of principle. Further, were it to be considered acceptable in principle, it is questionable on the evidence we have considered so far whether it is necessary and/or desirable.

---

44 *Zaw Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (Admin), para 84 and *R (on the application of Alan Lord) v secretary of State for the Home Department* [2003] EWHC 2073 (Admin).

45 Proceeds of Crime Act 2002, ss 330 and 331.

13.45 Furthermore, it is unclear whether any formulation of pre-suspicion information sharing would meet data protection requirements if the new provisions are interpreted in line with pre-existing case law.

13.46 We are asking consultees whether banks should be permitted to share information before a suspicion of money laundering has being formed or whether it would be inappropriate to allow them to do so. If consultees believe it is necessary or would be desirable, we welcome views on how provisions to share information below the suspicion threshold might be formulated which align with obligations under the GDPR and the Data Protection Act 2018.

Consultation Question 29.

13.47 Do consultees believe that sharing information by those in the regulated sector before a suspicion of money laundering has been formed is:

(1) necessary; and/or

(2) desirable; or

(3) inappropriate?

Consultation Question 30.

13.48 We invite consultees' views on whether pre-suspicion information sharing within the regulated sector, if necessary and/or desirable, could be articulated in a way which is compatible with the General Data Protection Regulation. We invite consultees' views on the following formulations:

(1) allowing information to be shared for the purposes of determining whether there is a suspicion that a person is engaged in money laundering;

(2) allowing information to be shared for the purpose of preventing and detecting economic crime;

(3) allowing information to be shared in order to determine whether a disclosure under sections 330 or 331 of the Proceeds of Crime Act 2002 would be required; or

(4) some other formulation which would be compatible with the UK's obligations under the General Data Protection Regulation?

Improving information sharing partnerships

Financial information sharing partnerships

13.49 There is a growing trend towards constructive information sharing partnerships between the public and private sector. In addition to JMLIT in the UK, the USA and Canada both have information sharing forums which bring together the private sector and law enforcement agencies. Between March and May 2017, three more financial information sharing partnerships ("FISPs") were introduced in Australia, Singapore and Hong Kong inspired by existing FISPs.[46] We will examine some of these existing financial information sharing partnerships in other jurisdictions below.

13.50 Maxwell and Artingstall have highlighted that the increasing number of reports of low intelligence value is a trend that is not isolated to the UK. The UK, USA, Hong Kong, Singapore, Australia and Canada have all seen an annual growth in reports with total suspicious transaction reporting growing at a rate of 11% per year. They argue that information sharing partnerships may be a useful tool to deal with the problem of reports of low intelligence value. [47]

Australia

13.51 The Fintel alliance in Australia allows for the exchange of intelligence in near real-time. This is achieved by combining the financial sector, non-government organisations, law enforcement agencies and national security agencies working side-by-side in one operational hub.[48] Its membership is broader in scope than that of JMLIT, encompassing a digital money transmitter, a money service bureau and multiple law enforcement agencies. Private sector to private sector information sharing is not permitted under Australian law. Information is sent and received through Australia's FIU (AUSTRAC).[49]

USA

13.52 The USA provides for two types of information sharing; private sector to private sector[50] and public sector to private sector.[51] The sharing of information between the public and private sectors operates under section 314(a) of the USA PATRIOT Act 2001. The provisions enable law enforcement agencies (including EU agencies) to request

---

46 Nick Maxwell and David Artingstall, Royal United Service Institute for Defence and Security Studies (RUSI), *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime* (October 2017) p 1. The Fintel Alliance in Australia, the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) in Singapore and the Fraud and Money Laundering Intelligence Taskforce (FMLIT) in Hong Kong.

47 Nick Maxwell and David Artingstall, Royal United Service Institute for Defence and Security Studies (RUSI), *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime* (October 2017) p 5.

48 http://www.austrac.gov.au/about-us/austrac/fintel-alliance (last accessed on 21 May 2018).

49 Nick Maxwell and David Artingstall, Royal United Service Institute for Defence and Security Studies (RUSI), *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime* (October 2017) p 15 to 16.

50 Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism Act (USA PATRIOT ACT) of 2001 (Public law 107-56 26 October 2001), s 314B.

51 Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism Act (USA PATRIOT ACT) of 2001 (Public law 107-56 26 October 2001, s 314A.

information from financial institutions concerning individuals or entities suspected of being involved in money laundering and terrorist financing. Requests for information are reportedly tightly focused and relate to significant investigations.[52]

13.53 Information sharing is also permitted on a voluntary basis between private entities under section 314(b) of the USA PATRIOT Act 2001. It allows for data sharing between financial institutions, regulatory authorities and law enforcement agencies in relation to specified unlawful activities (not "all-crimes").[53] Guidance clarifies that a financial institution participating in the section 314(b) program may share information relating to transactions that the official in the institution suspects may involve the proceeds of one or more specified unlawful activities ("SUAs"). Disclosures are protected by a "safe harbour" provision within section 314(b).[54] A financial institution must comply with the requirements of the implementing regulation, including provision of notice to FinCEN, taking reasonable steps to verify that the other financial institution has submitted the requisite notice, and restrictions on the use and security of information shared. Information obtained under this provision is not to be used for a wider/other purpose.[55]

Canada

13.54 Project PROTECT is a public-private partnership that uses SARs to target human trafficking for the purposes of sexual exploitation by focusing on the money laundering aspect of the crime.[56] In Canada, reporting entities have a legal obligation to submit a report to the FIU (FINTRAC) when they have reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering or terrorist activity financing offence. These suspicious transaction reports are analysed along with any other information and are disclosed to law enforcement agencies when the threshold for disclosure is met. Project PROTECT has a broader membership than JMLIT. Whilst it was originally limited to large domestic banks, its membership has expanded to include all major reporting entities alongside law enforcement agencies and its FIU (FINTRAC). The legislative framework in Canada does not allow for private sector to private sector information sharing.[57]

---

52 Neil Maxwell and D Artingstall, Royal United Service Institute for Defence and Security Studies (RUSI), *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime* (October 2017) p 14.

53 Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) Act of 2001 (Public law 107-56 October 26 2001, s 314(b) and 18 U S C § § 1956 and 1957.

54 FINCEN, Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbour of the USA PATRIOT Act 2009-G002 (June 16, 2009) https://www.fincen.gov/resources/statutes-regulations/guidance/guidance-scope-permissible-information-sharing-covered (last accessed on 20 May 2018).

55 Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism ACT (USA PATRIOT ACT) of 2001 (Public law 107-56 26 October 2001).

56 http://www.fintrac-canafe.gc.ca/emplo/psr-eng.asp (last accessed 29 June 2018).

57 Nick Maxwell and David Artingstall, Royal United Service Institute for Defence and Security Studies (RUSI), *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime* (October 2017) p 18.

Expanding JMLIT

13.55 During our pre-consultation discussions, stakeholders within the banking sector who are not JMLIT members expressed the view that JMLIT's membership should be expanded. They felt that there would be significant benefits to law enforcement agencies and the financial sector from widening participation.

13.56 There was also some support for expanding JMLIT's membership from a law enforcement stakeholder. One proposal was to expand JMLIT to create a more representative body encompassing the whole regulated sector. This could provide a better understanding of relevant intelligence through the sharing of information across multiple sectors. In addition, there are law enforcement agencies who are not included such as the Crown Prosecution Service and the Serious Fraud Office. As we discussed above, other jurisdictions have adopted a broader membership structure in their financial information sharing partnerships, for example Australia and Canada.

13.57 While there is significant stakeholder support for expanded membership, it is unclear at present whether the advantages to be gained outweigh the costs of making such a change. Additional reporting sectors and/or law enforcement agencies may provide a wider perspective on intelligence. Broader membership may also assist in the provision of feedback to reporters. However, we observe that the existing information sharing structure has been successful and appears to be working effectively. There may be disadvantages in including additional reporting sectors and/or law enforcement agencies if such a change rendered the current structure unwieldy or cumbersome.

13.58 Section 7 of the Crime and Courts Act 2013 does not appear to present any obstacle to expanding membership of JMLIT. It is a broad information gateway allowing for disclosure to the NCA for the purposes of any NCA function. It also provides protection from breach of confidence (or any other restriction on the disclosure of information) arising from a disclosure within this forum.[58]

13.59 In light of stakeholder views and the perceived advantages to broader representation, we invite consultees' views on whether there would be significant benefits flowing from the inclusion of additional reporting sectors and/or law enforcement agencies within the JMLIT scheme.

[58] Crime and Courts Act 2013, s7(8).

Consultation Question 31.

13.60 Do consultees believe that significant benefit would be derived from including any of the following within the JMLIT scheme operating under the gateway in section 7 of the Crime and Courts Act 2013:

(1) additional regulated sector members;

(2) the regulated sector as a whole; or

(3) an alternative composition not outlined in (1) or (2)?

Consultation Question 32.

13.61 Do consultees believe that there would be significant benefit to including other law enforcement agencies within the JMLIT scheme?

Consultation Question 33.

13.62 Do consultees believe that there would be significant benefit to including any other entities within the JMLIT scheme?

Chapter 14: Enhancing the consent regime and alternative approaches

OVERVIEW

14.1 The primary focus of the project is, as the terms of reference make clear, on reforms that can be achieved within the current legislative regime. In the preceding chapters, we have examined the most pressing problems and explored options to improve the current system.

14.2 It is important to note that during our initial fact-finding, there was strong support from some stakeholders for the retention of the consent regime, albeit with many proposals as to how it might be improved to render it more effective. The regime serves a clear and valuable purpose. Law enforcement agencies gain investigative opportunities created by authorised disclosures. Those with reporting obligations recognised this benefit and felt that the authorised disclosure exemption should be retained due to the protection it provides from criminal liability. We believe that the adjustments that we have proposed to the existing regime will improve efficiency and balance the interests of law enforcement agencies, reporters and those who are the subject of disclosures. We do not propose the removal of the consent regime and the arguments in its favour have already been considered in some detail. We advocate an enhanced model of consent to improve the overall efficiency of the system.

14.3 In this chapter, we look more broadly and consider what a non-consent model might look like. We do so not to argue for a removal of the regime, but so that the relative merits of the existing scheme may be better understood. We will also discuss how the consent regime might be enhanced by other measures that have not been considered in earlier Chapters and may be beneficial.

ALTERNATIVE MODELS TO SEEKING CONSENT

Removing the authorised disclosure exemption

14.4 As we have discussed in this paper, the principal advantage of a consent model is the opportunity provided to law enforcement agencies to investigate and potentially disrupt criminal activity at an early stage. To mitigate the risk of criminal liability for those in the regulated sector, particularly when criminal liability is triggered on the low threshold of suspicion, the authorised disclosure exemption provides comfort and legal protection to reporters. As the Law Society stated in 2016 in discussing the merits of retaining the existing regime:

> The defence afforded to those given consent was designed to counteract the far-reaching impact of the legislation. The 'all crimes approach' and the low threshold of ‘suspicion’ – unique among AML regimes in the world - necessitated protection for

reporters. The protection offered by the consent regime works to offer balance and to avoid over-criminalisation."[1]

14.5 In 2016, the Home Office and HM Treasury Action Plan considered removing the consent regime:

> The consent regime is inefficient and we will consider whether it should be removed. We envisage that it could be replaced with an intelligence-led approach, supported by information sharing through the Joint Money Laundering Intelligence Taskforce ("JMLIT") (see below). The statutory money laundering defence provided by the current consent regime would also be removed, although the POCA would be amended to ensure that reporters who fulfill their legal and regulatory obligations would not be criminalised. The Government would create powers to enable reporters to be granted immunity for taking specified courses of action (e.g. maintaining a customer relationship when to terminate it would alert the subject to the existence of an investigation). The Government would also legislate to provide a power for the National Crime Agency ("NCA") to oblige reporters to provide further information on a suspicious activity report ("SAR") where there is a need to do so.[2]

14.6 This proposal was not pursued and as noted above, we have found strong support for the existing consent regime, albeit with improvements, in pre-consultation discussions with stakeholders.

14.7 Any proposal to remove the authorised disclosure exemption would have to recognise that without such a defence the 2002 Act would expose those who will inevitably come into contact with criminal property (those in the regulated sector in particular) to a greater risk of criminal liability. Removing the scheme without replacement would remove a significant protection. It would also cause a substantial loss of intelligence for law enforcement agencies. Removal of the regime without either replacement or a significant rebalancing of the whole anti-money laundering regime seems untenable.

14.8 One alternative option would be to retain the suspicion threshold for reporting, but amend the threshold for the money laundering offences to require a higher degree of fault, such as knowledge. Such a scheme would not reduce the flow of valuable intelligence to the law enforcement agencies but would enhance the protection for those in the regulated sector against criminal liability.

14.9 Certain jurisdictions which do not have a consent regime do set the fault threshold for money laundering offences at a higher level. The USA sets the fault threshold at knowledge/intent for federal money laundering offences.[3] Ireland sets the fault threshold for the money laundering offences at knowledge, belief or recklessness as to whether

---

1 Response of the Law Society of England and Wales to the consultation issued by the Home Office and HM Treasury on the Action Plan for anti-money laundering and counter-terrorist finance – legislative proposals (June 2016).

2 Home Office and HM Treasury, Action Plan for anti-money laundering and counter-terrorist finance, para 2.8.

3 18 USC §1956(a)(1), §1956 (a)(2)(A) & (B), §1956(a)(1): §1956(a)(3), §1957.

or not the property is the proceeds of criminal conduct.[4] However, the accused is presumed to have known or believed, or have been reckless as to the property being criminal, unless the court or jury finds that there is a reasonable doubt to the contrary, taking into account 'the whole of the evidence'.[5]

14.10 In Canada, money laundering activities are criminalised on the basis that there must be an intent to conceal or convert the proceeds of crime, knowing or believing that all or part of that property or proceeds was obtained or derived directly or indirectly as a result of a predicate offence.[6]

14.11 Raising the fault threshold for the offences would offer some protection for those who will encounter criminal property in the course of their business or profession. However, it still exposes those with reporting obligations to a higher risk of criminal liability because of their likely contact with criminal property. Arguably they would be more at risk since the present scheme guarantees an exemption from criminal liability if the authorised disclosure has been made. Under this alternative model the only protection for the regulated sector employee would be that a criminal court would not find the relevant mens rea – knowledge – despite the employee having suspicion (as demonstrated by the fact of reporting).

14.12 If the threshold for reporting was retained at suspicion, it is questionable whether such a change would reduce the volume of reports of little use or value. Those reports which would previously have been made in the form of authorised disclosures would still be made as required disclosures. It would fall to the UK Financial Intelligence Unit ("UKFIU") and law enforcement agencies to identify those suspicious activity reports which required urgent attention.

14.13 One significant change would be that the bank would not be seeking consent to carry out the suspicious transaction. It would merely be alerting the UKFIU. The risk that criminal property would be "laundered" would therefore increase since activity on the suspicious accounts would not be suspended pending authorisation from the NCA. Provision could, however, be made to empower the NCA, law enforcement officers or a court to order the suspension of a transaction. For example, in Ireland a member of the Garda Síochána (not below the rank of superintendent) can direct a person, by notice in writing not to carry out any specified service or transaction for a period not exceeding seven days. The test for such a direction is whether it is "reasonably necessary" to enable the Garda to carry out "preliminary investigations" into whether or not there are "reasonable grounds to suspect that the service or transaction would, if it were to proceed, comprise or assist in money laundering or terrorist financing".[7]

14.14 In addition, a Judge of the District Court may order a person not to carry out any specified service or transaction for a period not exceeding 28 days.[8] The judge must be

---

4 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, s 7(1)(b).

5 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, s 11.

6 Criminal Code (CC), ss.354 (possession of proceeds), 355.2 (trafficking in proceeds), and 462.31 (laundering proceeds). Conversion or Transfer: CC, s.462.31

7 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, s 17(1).

8 Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, s 17(2).

satisfied (by information on oath of a member of the Garda Síochána) that, (a) there are reasonable grounds to suspect that the service or transaction would, if it were to proceed, comprise or assist in money laundering or terrorist financing, and (b) an investigation of a person for that money laundering or terrorist financing is taking place.

14.15 Importantly, the onus shifts to law enforcement agencies to take steps to suspend any transaction rather than the reporter.

14.16 In the light of that concern, for this model to function, there needs to be some way of identifying the most serious or urgent cases where money or other property is on the cusp of moving jurisdiction or otherwise changing ownership. Flagged or tiered reporting might be used to ensure that law enforcement agencies could identify the most urgent or serious cases. The Financial Intelligence Unit ("FIU") which processes these reports and/or the reporter could grade suspicious activity reports according to set criteria indicative of risk and urgency.

14.17 Australia does not operate a consent process. Their FIU (AUSTRAC) flags cases according to the nature of the alleged offence, risk or other material fact. Those that require urgent attention are made available to law enforcement agencies between one hour and one day of receipt.[9] This approach would arguably require greater intelligence analysis at FIU level and immediate action from law enforcement agencies.

14.18 The principal benefit of the non-consent model outlined above is that it would allow minimal disruption to legitimate economic activity without reducing the financial intelligence available to law enforcement agencies. The private sector would not have to make authorised disclosures and concerns about handling customers and clients would fall away. Transactions would continue unimpeded unless law enforcement agencies took further action.

14.19 There are, however, a number of disadvantages to this approach:

(1) it places the onus on the FIU to make the most pressing suspicious activity reports available to law enforcement agencies as quickly as possible. If the statutory notice period and moratorium periods were dispensed with, this would increase the risk of dissipation of the proceeds of crime. Transactions would not be paused automatically at the suspicion stage (instigated by the reporter due to the risk of criminal liability) and law enforcement agencies would need to act quickly.

(2) the scheme would be a new one and is not sought by those in the regulated sector. The authorised disclosure exemption provides clear legal protection for those with reporting obligations when they are dealing with criminal property. The process is well-defined and reporters know whether they are afforded a defence or not. Stakeholders were broadly unanimous in their support for the authorised disclosure exemption and feared its removal would create legal uncertainty.

---

9 FATF Annual Report (2014-2015). http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Australia-2015.pdf, p 50 (last accessed 18 June 2018).

(3) losing the protection of the authorised disclosure exemption might increase defensive reporting. The perception of greater exposure to criminal liability may have a negative impact on reporting behaviour.

(4) as we have previously discussed, civilian reporters may not be best placed to decide what should be a priority for law enforcement agencies. The application of suspicion has already proven to be problematic in the absence of statutory guidance. Asking reporters to flag their reports would also create an additional administrative burden.

(5) removal of the authorised disclosure exemption could negatively impact on the police and Crown Prosecution Service and their ability to investigate and prosecute money laundering. Currently where an individual suspects that property is the proceeds of crime, such property is in fact the proceeds of crime and the individual performs one of the acts prohibited under sections 327, 328 or 329 of POCA, they are at risk of criminal liability. As we identified in previous Chapters, in the absence of compelling evidence that the threshold is wrong, there are strong arguments for retaining the fault threshold at suspicion for the money laundering offences.

Consultation Question 34.

14.20 Do consultees believe that the consent regime should be retained? If not, can consultees suggest an alternative regime that would balance the interests of reporters, law enforcement agencies and those who are the subject of disclosures?

ALTERNATIVE APPROACHES TO THE CONSENT REGIME

14.21 In addition to our provisional proposals, we have considered other measures which may improve the existing regime.

Thematic reporting

14.22 In this paper, we have discussed suspicion-based reporting as a method of tackling money laundering and terrorist financing in some detail. This is not the only means of generating financial intelligence. Broadly, two methods have developed to combat money laundering and terrorism financing: the suspicion-based approach and an administrative or prescriptive approach.[10]

14.23 The suspicion-based approach encourages the assessment of risk by the individual reporter. However, one of problems created by a subjective suspicion test is that the intelligence received depends upon the judgement applied by an individual reporter. As we have identified above, better guidance on suspicion could help reporters make more reasonable, evidence-based judgements.

14.24 In contrast, the administrative approach requires reports to be made based on set criteria irrespective of suspicion. For example, a report could be based on the value of

[10] *Banks and Financial Crime* (2nd edition, 2016), para 7.06.

a transaction or where it took place. As we have discussed, due to the Financial Action Task Force ("FATF") recommendations and the requirements of the Fourth Money Laundering Directive ("4AMLD"), in England and Wales transactional reports[11] could only be deployed to supplement suspicion-based reporting and could not replace suspicion-based reporting entirely. At present, there is no provision allowing for supplemental targeted transaction reports.

14.25 Some jurisdictions deploy suspicion-based reporting alongside specific transaction reporting. Federal law in the USA requires the submission of certain transaction based reports in addition to suspicious activity reports. For example, submission of a Currency Transaction Report ("CTR") is required when a set threshold is reached.[12] Other examples of specific reporting obligations are those relating to the import or export of monetary instruments[13] and US citizens who hold foreign bank and financial accounts containing funds over a threshold amount.[14]

Geographic targeting orders

14.26 In addition to these specific transaction reports, there is greater flexibility under US federal law to target transactions in a particular location where there is a high risk of money laundering. The Director of FinCEN (the USA's Financial Intelligence Unit) is empowered to make a Geographic Targeting Order[15] ("GTO") where reasonable grounds exist for concluding that additional record keeping and reporting requirements are necessary to support the anti-money laundering system.[16] This gives FinCEN the means of targeting domestic financial institutions or businesses in a particular geographic area. In the absence of an extension a GTO lasts a maximum of 180 days.

14.27 GTOs have been used with some success to target specific locations, sectors and transactions which present a high risk of money laundering. In 1997, the El Dorado Task Force, a network of Federal, State and local law enforcement agencies in the USA benefited from intelligence obtained from a GTO which focused on cash transfers to Colombia over a threshold value of $750. The intended target for the GTO was a number of money service businesses that were believed to be funnelling proceeds of drug trafficking to source countries. The House of Representatives heard evidence that:

---

11 Reporting requirements tied to a specific type of transaction such a property purchase.

12 Federal law requires financial institutions to report currency (cash or coin) transactions over $10,000 conducted by, or on behalf of, one person, as well as multiple currency transactions that aggregate to be over $10,000 in a single day. See 31 CFR '1010.311 (formerly 31 CFR 103.22(b)(1)) [Financial institutions other than casinos]; 31 CFR '1021.311 (formerly 31 CFR 103.22(b)(2)) [Casinos] and 31 USC ' 5324(d).

13 Currency or monetary instruments reports ("CMIRs") 31 CFR 1010.340.

14 Foreign bank and financial accounts reporting ("FBAR") 31 USC 5314 and see FinCEN "Report Foreign Bank and Financial Accounts," https://www.fincen.gov/report-foreign-bank-and-financial-accounts (last accessed on 18 June 2018).

15 Pursuant to 31 USC 5326.

16 The Currency and Foreign Transactions Reporting Act of 1970 (commonly referred to as the Bank Secrecy Act) is the USA equivalent of Part 7 of the Proceeds of Crime Act 2002. It requires financial institutions to keep records, file reports of cash transactions above a threshold amount and report suspicious activity that might signify money laundering, tax evasion or other criminal activities. https://www.fincen.gov/resources/fincens-mandate-congress (last accessed on 16 May 2018).

virtually overnight the cartel instructed its people to stop using the remitters. The cartel's cash piled up, and when they tried to get the money out of the country by smuggling it out, the Customs Service began seizing it in record amounts.

14.28 As a result of the more stringent requirements imposed on money service businesses, a 30% fall in money transmitters overall business volume to Colombia was recorded. As a consequence, bulk smuggling of cash across the border increased to avoid the scrutiny being applied through money transmission businesses. This led to significant gains for customs agents who were able to seize funds. Overall there was a fourfold increase in cash seizure following the introduction of the GTO.[17]

14.29 GTOs have also been used to target specific criminal activity and the funds that flow from it. For example, a GTO was directed at armoured car services importing or exporting funds through specific locations to acquire additional identifying information on certain transactions to target the movement of cash for Mexican drug trafficking organisations.[18] A GTO was also issued requiring enhanced reporting and recordkeeping for electronics exporters in Miami.[19] Orders can be precise and limited in scope to achieve greater financial intelligence on a specific target.

14.30 GTOs have also been deployed requiring USA title insurance companies to identify the natural persons behind shell companies used to pay for high-end residential real estate in specific locations. This GTO deliberately targeted shell companies used to purchase luxury residential property. FinCEN considered the data and concluded that:[20]

> Within this narrow scope of real estate transactions covered by the GTOs, FinCEN data indicate that about 30 percent of reported transactions involve a beneficial owner or purchaser representative that was also the subject of a previous suspicious activity report. This corroborates FinCEN's concerns about this small segment of the market in which shell companies are used to buy luxury real estate in "all-cash" transactions. In addition, feedback from law enforcement agencies indicates that the reporting has advanced criminal investigations. The expanded GTOs will further help law enforcement agencies and inform FinCEN's future efforts to assess and combat the money laundering risks associated with luxury residential real estate purchases.

14.31 There is evidence to suggest that, in the US at least, GTOs are a useful tool to counter money laundering. FinCEN announced the renewal of existing orders targeting real estate transactions in February 2017 on the basis they produce valuable data assisting

---

17 Use by the Department of the Treasury of the geographic targeting order as a method to combat money laundering: hearing before the Subcommittee on General Oversight and Investigations of the Committee on Banking and Financial Services, House of Representatives, One Hundred Fifth Congress, first session, March 11, 1997.

18 https://www.fincen.gov/news/news-releases/fincen-awards-recognize-law-enforcement-success-stories-supported-bank-secrecy (last accessed 27 June 2018).

19 https://www.fincen.gov/news/news-releases/fincen-renews-geographic-targeting-order-gto-requiring-enhanced-reporting-and (last accessed 27 June 2018).

20 https://www.fincen.gov/news/news-releases/fincen-targets-shell-companies-purchasing-luxury-properties-seven-major (last accessed 27 June 2018).

law enforcement agencies to address money laundering.[21] In recent years, GTOs have been credited with helping to combat trade-based money laundering practices and drug trafficking related money laundering.[22]

GTOs or thematic reporting in the UK?

14.32 The consent regime in the UK could be supplemented by some thematic reporting in this way. There may, however, be less justification for geographic targeting given the that the UK is significantly smaller than the USA. Moreover, it is unclear at present whether there are locations within the UK in which particular activities relating to money laundering are specific to that location. However, targeted reporting would not preclude focusing on a particular location if a pattern or trend emerged. The purchase of property may be one example where location might be relevant.

14.33 The advantage of introducing some thematic reporting is that it would allow law enforcement agencies to target specific transactions, sectors or behaviour where there was a greater risk of money laundering and/or terrorist financing. It may circumvent some of the problems created by suspicion-based reporting, where the quality of the intelligence is dependent on the judgement of the reporter. The present system is based on the subjective judgment on the facts of each case. The targeted systems work on the assumption that generic factors – location, type of transaction etc – can be identified in advance as being those which are likely to point to criminal property being involved.

14.34 Targeted reporting may serve to address sectors which have difficulty applying the suspicion test and may be under-reporting. The UKFIU does not comment as to the relative volume of reports from each sector. They state in their Annual Report that it is for the sectors and their supervisors to assess if the volume of SARs submitted is proportionate to the risk their sectors faced.

14.35 However, the National Risk Assessment ("NRA") in 2017 identified that the volume of SARs from particular sectors was relatively low. The legal sector was referenced in one example:

> The 2015 NRA assessed that the number of SARs submitted by the legal sector was relatively low, and numbers have declined since that stage with independent legal professionals submitting 3,447 SARs in 2015/16.6 The UKFIU has engaged with the certain parts of the legal sector with a view to improving relationships and the quality of SAR submissions in the sector.
>
> In addition, the government has taken steps to address the risks arising from links between legal services and the property market through the introduction of Unexplained Wealth Orders in the Criminal Finances Act 2017 ("CFA"). Through this measure, those suspected of serious criminality can be required to explain wealth that

---

21 https://www.fincen.gov/news/news-releases/fincen-renews-real-estate-geographic-targeting-orders-identify-high-end-cash (last accessed on 21 May 2018).

22 Rena S. Miller and Liana W. Rosen, Congressional Research Service: Anti-Money Laundering: An Overview for Congress (1 March 2017) www.crs.gov (last accessed on 21 May 2018), p 7 to 8.

appears disproportionate to their income, providing law enforcement agencies with an additional tool for investigations around high-end money laundering…[23]

14.36 The creation of Unexplained Wealth Orders in the Criminal Finances Act 2017 perhaps provides a further justification for targeted transaction reporting and record keeping requirements. An Unexplained Wealth Order can be made by the High Court where the court is satisfied that:

(1) the respondent holds property of a value greater than £50,000;

(2) the respondent is a politically exposed person[24], or there are reasonable grounds for suspecting that he/she is or has been involved in serious crime (or a person connected with the respondent has been so involved); and

(3) there are reasonable grounds for suspecting that the known sources of the respondent's lawfully obtained income would have been insufficient for the purposes of enabling the respondent to obtain the property.

14.37 In relation to the first condition, targeted transaction reporting may be useful in identifying the existence of property which may be amenable to an Unexplained Wealth Order. For example, if law enforcement agencies were concerned about organised criminals using shell companies to invest in luxury properties, investigations currently rely on individual reporters making disclosures if they are suspicious. If suspicion is not applied consistently, it can create gaps in intelligence.

14.38 There may be some disadvantages to the introduction of transactional reporting. Such a change could negatively influence reporting behaviour. For example, levels of vigilance may fall if reporters interpreted such a change as reducing their individual responsibility for identifying risk. There is also a risk that transactional reporting would simply create more "noise" rather than intelligence. It is uncertain how many additional reports might be generated. However, unlike authorised disclosures which are resource intensive, transactional reporting would fall within the scope of required disclosures. These could be distributed to law enforcement agencies to allow them to perform their own searches in relation to new or existing lines of enquiry.

14.39 We invite consultees' views on whether some form of transactional reporting would improve the existing regime.

---

23 HM Treasury and Home Office, National risk assessment of money laundering and terrorist financing (2017), paras 7.13 (legal sector), 8.16 (estate agents), 9.31 (trust or company service providers), 11.17 (money service businesses).

24 Proceeds of Crime Act, s 362B(7). Politically exposed person means a person who is—(a) an individual who is, or has been, entrusted with prominent public functions by an international organisation or by a State other than the United Kingdom or another EEA State, (b) a family member of a person within paragraph (a), (c) known to be a close associate of a person within that paragraph, or (d) otherwise connected with a person within that paragraph.

Consultation Question 35.

14.40 Do consultees believe that a power to require additional reporting and record keeping requirements targeted at specific transactions would be beneficial?

Consultation Question 36.

14.41 Do consultees see value in introducing a form of Geographic Targeting Order?

Corporate criminal liability

14.42 Some stakeholders have suggested that there should be more emphasis on corporate criminal liability where individuals fail to report and it is commercially advantageous to the organisation to do so. In this section we will consider two different models of corporate liability that may address this issue; vicarious liability and strict liability where a commercial organisation fails to prevent an associate committing a criminal offence on their behalf.

Vicarious liability

14.43 Vicarious liability operates in a civil context by directly attributing blame for the acts of another. A corporation can be vicariously liable for the acts of its employees and agents. In *Mousell Bros v London and North Western Rly Co*, Atkin J. said:

> I think that the authorities cited by my Lord make it plain that while prima facie a principal is not to be made criminally responsible for the acts of his servants, yet the Legislature may prohibit an act or enforce a duty in such words as to make the prohibition or the duty absolute; in which case the principal is liable if the act is in fact done by his servants... [25]

14.44 One option for reform would be to introduce a criminal offence which held a commercial organisation to be liable where an employee or associate failed to report. Such an offence could provide for criminal liability for the corporate body where an employee or person fails to report a suspicion of money laundering or terrorist financing providing they are acting within the scope of their employment and the actions were intended, at least in part, to benefit the corporate entity.

14.45 Removing personal liability and holding the commercial organisation accountable could have a positive effect on the culture of an organisation. In order to avoid being held liable for the acts of its employees, an organisation would arguably seek to engage with the risks of facilitating money laundering or terrorism financing by improving standards of reporting. However, it is unclear whether defensive reporting would be reduced by

[25] [1917] 2 KB 845.

such an approach. The risk of liability for the organisation might in fact be a driver for greater volumes of reporting at the instigation of the corporate body.

14.46 However, the introduction of statutory liability in this way could operate unfairly and disproportionately. For example, a commercial organisation could be held liable despite having trained its employees and having proper procedures in place to ensure good reporting practices. A preferable method of imposing liability may be to create an offence which deals with the corporate failure to prevent an associate from committing a reporting offence.

Strict liability: failure to prevent

14.47 Whilst there are regulatory consequences for systemic failures, and corporate entities can be prosecuted for the principal money laundering offences, it is arguable that corporate entities should also be held liable for a general failure to prevent money laundering or terrorism financing. The focus on individual criminal liability can encourage devolved decision making about suspicious activity. Direct corporate responsibility may also have a greater impact on institutional behaviour. In addition, a failure to prevent model allows prosecutors to circumvent the identification principle which can create a bar to successful prosecutions:

> The difficulties of the identification doctrine are avoided by specifically providing which individuals associated with a company will trigger liability for the company by their actions.[26]

14.48 The failure to prevent model has been used in the Bribery Act 2010 and the Criminal Finances Act 2017 in relation to bribery and the facilitation of tax evasion offences. These offences focus on the culture of an organisation, its value and behaviours and "it is only very indirectly if at all that the company is being held responsible for the wrongs done by its agents".[27] If a failure to prevent model was adopted in relation to money laundering and/or terrorism financing, this could replace personal criminal liability unless an individual had the requisite knowledge of criminal property. However, where an individual failed to disclose a suspicion of criminal property, the corporate body would be liable for failing to prevent the associated person from committing an offence.

14.49 Sections 7 and 8 of the Bribery Act 2010 create a strict liability offence for commercial organisations where an associate pays a bribe to obtain or retain business or other advantage for the benefit of the organisation. The prosecution must prove that the associated person is guilty of bribery committed on the organisation's behalf. This is a strict liability offence, subject to a due diligence defence. It is a defence for the organisation to prove on the balance of probabilities that it had in place adequate procedures designed to prevent persons associated with it from undertaking such conduct.[28]

14.50 Part 3 of the Criminal Finances Act 2017 created corporate offences for failing to prevent facilitation of tax evasion offences by other persons. Section 45 creates an

---

[26] *Smith, Hogan and Ormerod's Criminal Law* (2018, 15th edition), p 264.

[27] *Smith, Hogan and Ormerod's Criminal Law* (2018, 15th edition), p 265.

[28] Bribery Act 2010, s 7(2).

offence of failing to prevent facilitation of UK tax evasion offences and section 46 relates to foreign tax evasion offences. These offences operate in a similar way although they do not require proof that the intention of the associated person in facilitating a tax evasion offence was to benefit the commercial organisation.

14.51 In both cases, safeguards are built in to the offences, for example any prosecution requires the consent of the DPP or the Director of SFO.[29] The Secretary of State has also published guidance to assist commercial organisations with creating adequate procedures to prevent bribery.[30] Similarly guidance has been issued in relation to procedures that relevant bodies can put in place to prevent persons acting in the capacity of an associated person from committing UK tax evasion facilitation offences or foreign tax evasion facilitation offences.[31]

14.52 In 2017, the Ministry of Justice consulted on reform of the law on corporate liability for economic crime. In particular, the consultation called for evidence on whether the failure to prevent model ought to be extended to apply to money laundering. The views of consultees following this call for evidence are awaited.[32]

14.53 If a failure to prevent model was used in the context of money laundering, a commercial organisation whose associates failed to report suspicions of criminal property could be held criminally liable. This would be subject to a due diligence defence, where an organisation could demonstrate on the balance of probabilities that it had taken reasonable measures to ensure appropriate reporting. This model avoids the unfairness created by holding the corporate body vicariously liable for the acts of an associate despite the fact that they had taken all reasonable steps to ensure that suspicious activity was reported. However, it would arguably have a similar impact on corporate culture by creating a powerful incentive to put in place adequate procedures.

Consultation Question 37.

14.54 Do consultees believe that consideration should be given to a new offence whereby a commercial organisation would be criminally liable for their employees' or associates' failure to report suspicions of money laundering or terrorist financing?

---

29 Bribery Act 2010, s 10(1) and Criminal Finances Act 2017, s 49(2).

30 Bribery Act 2010, s 9. Ministry of Justice, The Bribery Act 2010 Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing (2011) https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf (last accessed 19 June 2018).

31 Criminal Finances Act 2017, s 47. HM Revenue and Customs Tackling tax evasion: Government guidance for the corporate offences of failure to prevent the criminal facilitation of tax evasion (2017). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/672231/Tackling-tax-evasion-corporate-offences.pdf (last accessed 19 June 2018).

32 Ministry of Justice, Corporate Liability for Economic Crime: Call for Evidence (2017) Cm 9370 https://www.gov.uk/government/consultations/corporate-liability-for-economic-crime-call-for-evidence (last accessed 19 June 2018).

Consultation Question 38.

14.55 Do consultees believe that consideration should be given to introducing an offence for a commercial organisation to fail to take reasonable measures to ensure its associates reported suspicions of criminal property?

COMMISSION OF INQUIRY INTO STATE CAPTURE

Chapter 15: Consultation Questions

Consultation Question 1.

15.1 Do consultees agree that we should maintain the "all crimes" approach to money laundering by retaining the existing definition of "criminal conduct" in section 340 of the Proceeds of Crime Act 2002?

15.2 If not, do consultees believe that one of the following approaches would be preferable?

(1) a serious crimes approach, whether based on lists of offences or maximum penalty;

(2) retaining an all crimes approach for the money laundering offences but requiring SARS only in relation to "serious crimes" (to be defined by category and or sentence as discussed above). This could be achieved by extending the reasonable excuse defence to those who do not report, for example, suspected non-imprisonable crimes or those crimes listed on a schedule; or

(3) providing the opportunity to the regulated sector to draw to the attention of the FIU any non-serious cases, whilst maintaining a required disclosure regime for offences on a schedule of serious offences listed in one of the ways identified above.

[Paragraph 5.19]

Consultation Question 2.

15.3 We would value consultees' views on whether suspicion should be defined for the purposes of Part 7 of the Proceeds of Crime Act 2002? If so, how could it be defined?

[Paragraph 9.8]

Consultation Question 3.

15.4 We provisionally propose that POCA should contain a statutory requirement that Government produce guidance on the suspicion threshold. Do consultees agree?

[Paragraph 9.18]

Consultation Question 4.

15.5 We provisionally propose that the Secretary of State should introduce a prescribed form pursuant to section 339 of the Proceeds of Crime Act 2002 for Suspicious Activity Reports which directs the reporter to provide grounds for their suspicion. Do consultees agree?

[Paragraph 9.21]

Consultation Question 5.

15.6 We would welcome consultees' views on whether there should be a single prescribed form, or separate forms for each reporting sector.

[Paragraph 9.22]

Consultation Question 6.

15.7 We provisionally propose that the threshold for required disclosures under sections 330, 331 and 332 of the Proceeds of Crime Act 2002 should be amended to require reasonable grounds to suspect that a person is engaged in money laundering. Do consultees agree?

[Paragraph 9.63]

Consultation Question 7.

15.8 If consultees agree that the threshold for required disclosures should be amended to reasonable grounds for suspicion, would statutory guidance be of benefit to reporters in applying this test?

[Paragraph 9.64]

Consultation Question 8.

15.9 We provisionally propose that the suspicion threshold for the money laundering offences in sections 327, 328, 329 and 340 of the Proceeds of Crime Act 2002 should be retained. Do consultees agree?

[Paragraph 9.65]

Consultation Question 9.

15.10 We provisionally propose that it should be a defence to the money laundering offences in sections 327, 328 and 329 if an individual in the regulated sector has no reasonable grounds to suspect that property is criminal property within the meaning of section 340 of the Proceeds of Crime Act 2002. Do consultees agree?

[Paragraph 9.66]

Consultation Question 10.

15.11 Does our summary of the problems presented by mixed funds accord with consultees' experience of how the law operates in practice?

[Paragraph 10.42]

COMMISSION OF INQUIRY INTO STATE CAPTURE

Consultation Question 11.

15.12 We provisionally propose that sections 327, 328 and 329 of POCA should be amended to provide that no criminal offence is committed by a person where:

(1) they are an employee of a credit institution;

(2) they suspect [*or if our earlier proposal in Chapter 9 is accepted have reasonable grounds to suspect*] that funds in their possession constitute a person's benefit from criminal conduct;

(3) the suspicion [*or if our earlier proposal in Chapter 9 is accepted reasonable grounds to suspect*] relates only to a portion of the funds in their possession;

(4) the funds which they suspect [*or if our earlier proposal in Chapter 9 is accepted have reasonable grounds to suspect*] constitute a person's benefit from criminal conduct are either:

(a) transferred to an account within the same credit institution; or

(b) the balance is not allowed to fall below the level of the suspected funds;

(5) they conduct the transaction in the course of business in the regulated sector (as defined in Schedule 9 of the Proceeds of Crime Act 2002); and

(6) the transfer is done with the intention of preserving criminal property.

15.13 Do consultees agree?

[Paragraph 10.43]

Consultation Question 12.

15.14 We provisionally propose that statutory guidance should be issued to provide examples of circumstances which may amount to a reasonable excuse not to make a required and/or an authorised disclosure under Part 7 of the Proceeds of Crime Act 2002. Do consultees agree?

[Paragraph 11.7]

Consultation Question 13.

15.15 It is our provisional view that introducing a minimum financial threshold for required and authorised disclosures would be undesirable. Do consultees agree?

[Paragraph 11.20]

Consultation Question 14.

15.16 Do consultees believe that the threshold amount in section 339A of the Proceeds of Crime Act 2002 should be raised? If so, what is the appropriate threshold amount?

[Paragraph 11.21]

Consultation Question 15.

15.17 We provisionally propose that any statutory guidance issued should indicate that the moving criminal funds internally within a bank or business with the intention of preserving them may amount to a reasonable excuse for not making an authorised disclosure within the meaning of sections 327(2)(b), 328(2)(b) and 329(2)(b) of the Proceeds of Crime Act 2002.

15.18 Do consultees agree?

[Paragraph 11.23]

Consultation Question 16.

15.19 Do consultees agree that there is insufficient value in required or authorised disclosures to justify duplicate reporting where a report has already been made to another law enforcement agency (in accordance with the proposed guidance)?

[Paragraph 11.28]

Consultation Question 17.

15.20 We provisionally propose that statutory guidance be issued indicating that a failure to make a required disclosure where a report has been made directly to a law enforcement agency on the same facts (in accordance with proposed guidance on reporting routes) may provide the reporter with a reasonable excuse within the meaning of sections 330(6)(a), 331(6) and 332(6) of the Proceeds of Crime Act 2002. Do consultees agree?

[Paragraph 11.30]

Consultation Question 18.

15.21 We provisionally propose that a short-form report should be prescribed, in accordance with section 339 of the Proceeds of Crime Act 2002, for disclosures where information is already in the public domain. Do consultees agree?

[Paragraph 11.37]

Consultation Question 19.

15.22 We provisionally propose that statutory guidance should be issued indicating that it may amount to a reasonable excuse to a money laundering offence not to make an authorised disclosure under sections 327(2), 328(2) and 329(2) of the Proceeds of Crime Act 2002 where funds are used to purchase a property or make mortgage payments on a property within the UK. Do consultees agree?

[Paragraph 11.41]

Consultation Question 20.

15.23 We provisionally propose that the obligation to make a required disclosure in accordance with sections 330, 331 and 332 of the Proceeds of Crime Act 2002 in these circumstances should remain? Do consultees agree?

[Paragraph 11.42]

Consultation Question 21.

15.24 We provisionally propose that reporters should be able to submit one SAR for:

(1) multiple transactions on the same account as long as a reasonable description of suspicious activity is provided; and/or

(2) multiple transactions for the same company or individual.

15.25 Do consultees agree?

[Paragraph 11.45]

Consultation Question 22.

15.26 Do consultees agree that banks should not have to seek consent to pay funds back to a victim of fraud where they have filed an appropriate report to Action Fraud?

[Paragraph 11.49]

Consultation Question 23.

15.27 Do consultees believe that there is value in disclosing historical crime?

[Paragraph 11.52]

Consultation Question 24.

15.28 How long after the commission of a criminal offence would a disclosure be considered historical for the purposes of law enforcement agencies?

[Paragraph 11.53]

Consultation Question 25.

15.29 We provisionally propose that statutory guidance be issued indicating that where a transaction has no UK nexus, this may amount to a reasonable excuse not to make a required or authorised disclosure. Do consultees agree?

[Paragraph 11.56]

Consultation Question 26.

15.30 Are there are any additional types of SAR under POCA which are considered to be of little value or utility that we have not included?

[Paragraph 11.59]

Consultation Question 27.

15.31 We provisionally propose that there should be a requirement in POCA that Government produces guidance on the concept of "appropriate consent" under Part 7 of the Act. Do consultees agree?

[Paragraph 12.28]

Consultation Question 28.

15.32 Based on their experience, do consultees believe that statutory guidance on arrangements with prior consent within the meaning of section 21ZA of the Terrorism Act 2000 would be beneficial?

[Paragraph 12.29]

Consultation Question 29.

15.33 Do consultees believe that sharing information by those in the regulated sector before a suspicion of money laundering has been formed is:

(1) necessary; and/or

(2) desirable; or

(3) inappropriate?

[Paragraph 13.47]

Consultation Question 30.

15.34 We invite consultees' views on whether pre-suspicion information sharing within the regulated sector, if necessary and/or desirable, could be articulated in a way which is compatible with the General Data Protection Regulation. We invite consultees' views on the following formulations:

(1) allowing information to be shared for the purposes of determining whether there is a suspicion that a person is engaged in money laundering;

(2) allowing information to be shared for the purpose of preventing and detecting economic crime;

(3) allowing information to be shared in order to determine whether a disclosure under sections 330 or 331 of the Proceeds of Crime Act 2002 would be required; or

(4) some other formulation which would be compatible with our obligations under the General Data Protection Regulation?

[Paragraph 13.48]

Consultation Question 31.

15.35 Do consultees believe that significant benefit would be derived from including any of the following within the JMLIT scheme operating under the gateway in section 7 of the Crime and Courts Act 2013:

(1) additional regulated sector members;

(2) the regulated sector as a whole; or

(3) an alternative composition not outlined in (1) or (2)?

[Paragraph 13.60]

Consultation Question 32.

15.36 Do consultees believe that there would be significant benefit to including other law enforcement agencies within the JMLIT scheme?

[Paragraph 13.61]

Consultation Question 33.

15.37 Do consultees believe that there would be significant benefit to including any other entities within the JMLIT scheme?

[Paragraph 13.62]

Consultation Question 34.

15.38 Do consultees believe that the consent regime should be retained? If not, can consultees conceive of an alternative regime that would balance the interests of reporters, law enforcement agencies and those who are the subject of disclosures?

[Paragraph 14.20]

Consultation Question 35.

15.39 Do consultees believe that a power to require additional reporting and record keeping requirements targeted at specific transactions would be beneficial?

[Paragraph 14.40]

Consultation Question 36.

15.40 Do consultees see value in introducing a form of Geographic Targeting Order?

[Paragraph 14.41]

Consultation Question 37.

15.41 Do consultees believe that consideration should be given to a new offence whereby a commercial organisation would be criminally liable for their employees or associates failure to report suspicions of money laundering or terrorist financing?

[Paragraph 14.54]

Consultation Question 38.

15.42 Do consultees believe that consideration should be given to introducing an offence for a commercial organisation to fail to take reasonable measures to ensure its associates reported suspicions of criminal property?

[Paragraph 14.55]

Appendix 1: List of Acronyms

AML – Anti-Money Laundering

BACS - Bankers' Automated Clearing Services

CCAB – consultative committee of accountancy bodies

CHAPS - Clearing House Automated Payment System

CFT – Countering the Financing of Terrorism

DAML – Defence against money laundering

DATF – Defence against terrorist financing

FIN-NET – Financial Crime Information Network

FIU – Financial Intelligence Unit

FPSL – Faster Payment Scheme Limited

FTFIU – National Terrorism Financial Intelligence Unit

JMLIT – Joint Money Laundering Intelligence Taskforce

JMLSG – Joint money laundering steering group

ML – Money Laundering

POCA – Proceeds of Crime Act 2002

SIS – Shared intelligence service

SOI – Subject of interest

4AMLD – Fourth Anti-Money Laundering Directive

Appendix 2: Current end users with 'direct' access

POLICE FORCES

2.1 Avon and Somerset

2.2 Bedfordshire

2.3 British Transport Police

2.4 Cambridgeshire

2.5 Cheshire

2.6 City of London

2.7 Cleveland

2.8 Cumbia

2.9 Derbyshire

2.10 Devon and Cornwall

2.11 Dorset

2.12 Durham

2.13 Dyfed-Powys

2.14 Essex

2.15 Gloucestershire

2.16 Greater Manchester

2.17 Gwent

2.18 Hampshire

2.19 Herefordshire

2.20 Humberside

2.21 Kent

2.22 Lancashire

2.23 Leicestershire

2.24 Lincolnshire

2.25 Merseyside

2.26 Metropolitan Police Service

2.27 Ministry of Defence Police

2.28 Norfolk

2.29 Northamptonshire

2.30 Northumbria

2.31 North Wales

2.32 North Yorkshire

2.33 Nottinghamshire

2.34 Police Scotland

2.35 Police Service of Northern Ireland.

2.36 South Wales

2.37 Staffordshire

2.38 Suffolk

2.39 Surrey

2.40 Sussex

2.41 Thames Valley

2.42 Warwickshire

2.43 West Mercia

2.44 West Midlands

2.45 Wiltshire

Multi-agency teams and other agencies

2.46 Eastern Region Special Operations Unit

2.47 East Midlands RART

2.48 London RART

2.49 North East RART

2.50 North West RART

2.51 South East RART

2.52 South West RART

2.53 Wales RART

2.54 West Midlands RART

2.55 Crown Office, Civil recovery unity, Scotland

2.56 Department for Business, Energy and Industrial Strategy

2.57 Department for Environment, Food and Rural Affairs

2.58 Department for Work and Pensions

2.59 Environment agency

2.60 Financial Conduct Authority

2.61 Gambling Commission

2.62 HM Revenue and Customs

2.63 Home Office

2.64 National Crime Agency

2.65 National Port Analysis Centre

2.66 NHS Protect

2.67 Northern Ireland Department for Social Development

2.68 Northern Ireland Environment Agency

2.69 Serious Fraud Office. [1]

[1] National Crime Agency, Suspicious Activity Reports (SARs) Annual Report 2017, p 53

Appendix 3: Government departments, organisations and individuals consulted

3.1 This appendix lists the government departments, organisations and individuals with whom we have consulted during our initial consultation and whose views have informed our provisional conclusions and consultation questions.

3.2 **Government departments**

(1) Attorney General's Office

(2) Home Office

(3) Her Majesty's Revenue and Customs

(4) Her Majesty's Treasury

3.3 **Agencies, police and prosecuting authorities**

(1) Crown Prosecution Service

(2) Metropolitan Police Service

(3) City of London Police Service

(4) National Crime Agency

(5) UK Financial Intelligence Unit

(6) National Terrorist Financial Investigation Unit

(7) National Police Chiefs' Council

3.4 **Individuals and members of the judiciary**

(1) Jonathan Fisher QC (Bright Line Law)

(2) Paul Downes QC (Quadrant Chambers)

(3) Joanna Ludlam (Baker and Mackenzie)

(4) Daren Allen (Denton)

(5) Charlotte Hill (Covington and Burling)

(6) Liz Campbell (Durham University)

(7) Max Hill QC (Red Lion Chambers)

(8) David Artingstall (RUSI)

(9) James London (FCA)

(10) Laura Neff (AAT)

(11) Mark Skinner (Gambling Commission)

(12) Simon Garrod (CILEX)

(13) Caroline Sumner (R3 (insolvency practitioners))

(14) Samantha McDonanugh (CIMA)

(15) David Stevens (ICAEW)

(16) Collette Best (Solicitors Regulation Authority)

(17) Helena Mumdzjana (The Law Society)

(18) Professor Michael Levi (Cardiff University)

(19) Professor Sarah Kebbell (University of Sheffield)

(20) Dr Collin King (University of Sussex)

(21) Jacqueline Harvey (Northumbria University)

(22) Professor Peter Alldridge (Queen Mary, University of London)

(23) Dr Gauri Sunha (Kingston University)

(24) Miriam Goldby (Queen Mary, University of London)

(25) Dr Anna Bradshaw (Peters and Peters)

(26) Jonathan Grimes (Kingsley Napely)

(27) Anita Clifford (Bright Line Law)

(28) Natasha Ruarks (Bright Line Law)

(29) Neil Swift (Peters and Peters)

(30) Cherie Spinks (Simmons and Simmons)

(31) Richard Saynor (23 Essex Street)

(32) Kennedy Talbot QC (33 Chancery Lane)

(33) Shahmeem Purdasy (General Counsel, UK Finance)

(34) Katie Brandrith-Holmes (UK Finance)

(35) Fred Kelly (Barclays)

(36) Joe Smith (Barclays)

(37) Sinead Goss (Citibank)

(38) Helen Ratcliffe (HSBC)

(39) Mark Reynolds (HSBC)

(40) Mike Venn (HSBC)

(41) Daniel Rawsterne (JP Morgan)

(42) Dan White (JP Morgan)

(43) Adam Bond (JP Morgan)

(44) Kelly Jones (JP Morgan)

(45) Ellie Sanner (Lloyds Banking)

(46) Tina Blocksidge (Lloyds Banking Group)

(47) Jonathan Wickett (Lloyds Banking Group)

(48) Ina Jahn (Lloyds Banking)

(49) Jacky Murnane (Metro Bank)

(50) Tim Care (Metro Bank)

(51) James Thurgood (Metro Bank)

(52) Andrew Waters (Nationwide)

(53) Aga Polcyn (Morgan Stanley)

(54) Natalie Davidson (Morgan Stanley)

(55) Ann Doan (Norinchuckin Bank)

(56) Tom Littlechild (Santander UK)

(57) Andrew Lall (The Royal Bank of Scotland)

(58) James Kent (The Royal Bank of Scotland)

(59) Louise Engal (The Royal Bank of Scotland)

(60) Nicola Hannah (The Royal Bank of Scotland)

COMMISSION OF INQUIRY
INTO STATE CAPTURE

Appendix 4: The regulated sector

The Money Laundering Regulations 2007 SI 2157/2007

3.—(1) Subject to Regulation 4, these Regulations apply to the following persons acting in the course of business carried on by them in the United Kingdom ("relevant persons")—

(a) credit institutions;

(b) financial institutions;

(c) auditors, insolvency practitioners, external accountants and tax advisers;

(d) independent legal professionals;

(e) trust or company service providers;

(f) estate agents;

(g) high value dealers;

(h) casinos.

(2) "Credit institution" means—

(a)a credit institution as defined in Article 4(1)(a) of the banking consolidation directive; or

(b)a branch (within the meaning of Article 4(3) of that directive) located in an EEA state of an institution falling within sub-paragraph (a) (or an equivalent institution whose head office is located in a non-EEA state) wherever its head office is located,

when it accepts deposits or other repayable funds from the public or grants credits for its own account (within the meaning of the banking consolidation directive).

(3) "Financial institution" means—

(a)an undertaking, including a money service business, when it carries out one or more of the activities listed in points 2 to 12 and 14 of Annex 1 to the banking consolidation directive (the relevant text of which is set out in Schedule 1 to these Regulations), other than—

(i) a credit institution;

(ii) an undertaking whose only listed activity is trading for own account in one or more of the products listed in point 7 of Annex 1 to the banking consolidation directive where the undertaking does not have a customer,

and, for this purpose, "customer" means a third party which is not a member of the same group as the undertaking;

(b) an insurance company duly authorised in accordance with the life assurance consolidation directive, when it carries out activities covered by that directive;

(c) a person whose regular occupation or business is the provision to other persons of an investment service or the performance of an investment activity on a professional basis, when providing or performing investment services or activities (within the meaning of the markets in financial instruments directive(1)), other than a person falling within Article 2 of that directive;

(d) a collective investment undertaking, when marketing or otherwise offering its units or shares;

(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9th December 2002(2) on insurance mediation, with the exception of a tied insurance intermediary as mentioned in Article 2(7) of that Directive, when it acts in respect of contracts of long-term insurance within the meaning given by article 3(1) of, and Part II of Schedule 1 to, the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001(3);

(f) a branch located in an EEA state of a person referred to in sub-paragraphs (a) to (e) (or an equivalent person whose head office is located in a non-EEA state), wherever its head office is located, when carrying out any activity mentioned in sub-paragraphs (a) to (e);

(g) the National Savings Bank;

(h) the Director of Savings, when money is raised under the auspices of the Director under the National Loans Act 1968(4).

(4) "Auditor" means any firm or individual who is a statutory auditor within the meaning of Part 42 of the Companies Act 2006(5) (statutory auditors), when carrying out statutory audit work within the meaning of section 1210 of that Act.

(5) Before the entry into force of Part 42 of the Companies Act 2006 the reference in paragraph (4) to—

(a)a person who is a statutory auditor shall be treated as a reference to a person who is eligible for appointment as a company auditor under section 25 of the Companies Act 1989(6) (eligibility for appointment) or article 28 of the Companies (Northern Ireland) Order 1990(7); and

(b)the carrying out of statutory audit work shall be treated as a reference to the provision of audit services.

(6) "Insolvency practitioner" means any person who acts as an insolvency practitioner within the meaning of section 388 of the Insolvency Act 1986(8) (meaning of "act as insolvency practitioner") or article 3 of the Insolvency (Northern Ireland) Order 1989(9).

(7) "External accountant" means a firm or sole practitioner who by way of business provides accountancy services to other persons, when providing such services.

(8) “Tax adviser” means a firm or sole practitioner who by way of business provides advice about the tax affairs of other persons, when providing such services.

(9) “Independent legal professional” means a firm or sole practitioner who by way of business provides legal or notarial services to other persons, when participating in financial or real property transactions concerning—

(a)the buying and selling of real property or business entities;

(b)the managing of client money, securities or other assets;

(c)the opening or management of bank, savings or securities accounts;

(d)the organisation of contributions necessary for the creation, operation or management of companies; or

(e)the creation, operation or management of trusts, companies or similar structures,

and, for this purpose, a person participates in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

(10) “Trust or company service provider” means a firm or sole practitioner who by way of business provides any of the following services to other persons—

(a)forming companies or other legal persons;

(b)acting, or arranging for another person to act—

(i)as a director or secretary of a company;

(ii)as a partner of a partnership; or

(iii)in a similar position in relation to other legal persons;

(c)providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement;

(d)acting, or arranging for another person to act, as—

(i)a trustee of an express trust or similar legal arrangement; or

(ii)a nominee shareholder for a person other than a company whose securities are listed on a regulated market,

when providing such services.

(11) “Estate agent” means—

(a)a firm; or

(b)sole practitioner,

who, or whose employees, carry out estate agency work (within the meaning given by section 1 of the Estate Agents Act 1979(10) (estate agency work)), when in the course of carrying out such work.

(12) “High value dealer” means a firm or sole trader who by way of business trades in goods (including an auctioneer dealing in goods), when he receives, in respect of any transaction, a payment or payments in cash of at least 15,000 euros in total, whether the transaction is executed in a single operation or in several operations which appear to be linked.

(13) “Casino” means the holder of a casino operating licence and, for this purpose, a “casino operating licence” has the meaning given by section 65(2) of the Gambling Act 2005(11) (nature of licence).

(14) In the application of this regulation to Scotland, for “real property” in paragraph (9) substitute “heritable property”.

COMMISSION OF INQUIRY INTO STATE CAPTURE

COMMISSION OF INQUIRY
INTO STATE CAPTURE

PH-628

GDPR cookie consent

Agree and close

This website uses cookies to enhance your browsing experience and collect information on how you use the website. To consent to our use of cookies, click on the 'Agree and close' button.

National Economic Crime Centre

The National Economic Crime Centre (NECC) has been created to deliver a step change in the UK's response to, and impact on, economic crime. For the first time, the NECC brings together law enforcement and justice agencies, government departments, regulatory bodies and the private sector with a shared objective of driving down serious organised economic crime, protecting the public and safeguarding the prosperity and reputation of the UK as a financial centre.

NECC

NATIONAL ECONOMIC CRIME CENTRE

Improving the UK's response to economic crime

The NECC will coordinate and task the UK's response to economic crime, harnessing intelligence and capabilities from across the public and private sectors to tackle economic crime in the most effective way.

It will jointly identify and prioritise the most appropriate type of investigations, whether criminal, civil or regulatory to ensure maximum impact. It will seek to maximise new powers, for example Unexplained Wealth Orders and Account Freezing Orders, across all agencies to tackle the illicit finance that funds and enables all forms of serious and organised crime.

The NECC will ensure that criminals defrauding British citizens, attacking UK industry and abusing UK financial services are effectively pursued; that the UK's industries and government agencies know how to prevent economic crime; and that the UK's citizens are better protected.

Agencies involved in the NECC

The NECC launched on 31 October 2018 with officers or representatives from the agencies below.

NCA National Crime Agency · SFO serious fraud office · FCA Financial Conduct Authority · City of London Police · HM Revenue & Customs · CPS · Home Office

As the NECC evolves throughout 2019 and beyond it will build wider partnerships across the public sector, with regulators and the private sector, particularly with those businesses at risk from economic crime.

Joint Money Laundering Intelligence Taskforce

PH-629

The NECC includes the well established Joint Money Laundering Intelligence Taskforce (JMLIT). JMLIT is a partnership between law enforcement and the financial sector to exchange and analyse information relating to money laundering and wider economic threats.

jmlit
Joint Money Laundering Intelligence Taskforce
Tackling financial crime together

The taskforce consists of:

- over 40 financial institutions
- the Financial Conduct Authority
- Cifas
- five law-enforcement agencies: the NCA, HMRC, the SFO, the City of London Police, and the Metropolitan Police Service.

JMLIT is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015, and is considered internationally to be an example of best practice.

If the UK is to tackle high-end money laundering schemes which are most commonly complex, multi-institutional, and multi-jurisdictional, then a forum to share information on new typologies, existing vulnerabilities, and live tactical intelligence, is essential.

Successes of JMLIT

Since its inception, JMLIT has supported and developed over 500 law enforcement investigations which has directly contributed to over 130 arrests and the seizure or restraint of over £13m.

Through this collaboration, JMLIT private sector members have identified over 5,000 suspect accounts linked to money laundering activity, and commenced over 3,500 of their own internal investigations, while also continuing to develop and enhance their systems and controls for mitigating the threat of financial crime.

Financial sector-led expert working groups provide a platform for members to discuss current or emerging threats, and to identify innovative ways of collectively combating these threats. As a result, over 30 'JMLIT Alert' reports have been shared with the wider financial industry to assist in focussing the identification and implementation of transactional monitoring system queries, in turn helping to mitigate the criminal methodologies used to exploit the UK's financial system.

Future development of JMLIT

There has been a real willingness within the banking sector to share information through the JMLIT to combat economic crime. The NCA is working with colleagues from overseas law enforcement agencies to help inform the development of similar partnerships in a number of key partner jurisdictions around the world.

Continued commitment and support from both sides will allow us to work together to construct a new, wider, "whole system" approach, which will enable the private sector to act as a more effective first line of defence against economic crime.

Related publications

(/who-we-are/publications/391-sars-in-action-november-2019) SARs In Action November 2019 (/who-we-are/publications/391-sars-in-action-november-2019) **New Popular**

(/who-we-are/publications/388-glossary-codes-and-reporting-routes-new) SAR Glossary Codes and Reporting Routes (2019) (/who-we-are/publications/388-glossary-codes-and-reporting-routes-new) **Popular**

(/who-we-are/publications/323-public-private-threat-update-2019-economic-crime) Public Private Threat Update 2019 - Economic Crime (/who-we-are/publications/323-public-private-threat-update-2019-economic-crime) **Popular**

2018 SARs Annual Report (/who-we-are/publications/256-2018-sars-annual-report) **Popular**

(/who-we-are/publications/256-2018-sars-annual-report)

(/who-we-are/publications/242-national-economic-crime-centre-working-together-to-protect-the-public-prosperity-and-the-uk-s-reputation)

National Economic Crime Centre: Working together to protect the public, prosperity and the UK's reputation (/who-we-are/publications/242-national-economic-crime-centre-working-together-to-protect-the-public-prosperity-and-the-uk-s-reputation)

Popular

Economic crime threats

Money laundering and illicit finance (/what-we-do/crime-threats/money-laundering-and-terrorist-financing)

Fraud (/what-we-do/crime-threats/fraud-and-economic-crime)

Bribery, corruption and sanctions evasion (/what-we-do/crime-threats/bribery-corruption-and-sanctions-evasion)

Crime threats (https://nationalcrimeagency.gov.uk//what-we-do/crime-threats)

Latest vacancies

There are currently no open vacancies related to this article. Click on the button below to view all vacancies.

All current vacancies (https://nationalcrimeagency.gov.uk/careers/vacancies)

Share this page: (https://www.facebook.com/sharer.php?u=https%3A%2F%2Fnationalcrimeagency.gov.uk%2Fwhat-we-do%2Fnational-economic-crime-centre) (https://twitter.com/intent/tweet?text=https%3A%2F%2Fnationalcrimeagency.gov.uk%2Fwhat-we-do%2Fnational-economic-crime-centre) (mailto:?subject=National%20Crime%20Agency%20website&body=https%3A%2F%2Fnationalcrimeagency.gov.uk%2Fwhat-we-do%2Fnati crime-centre)

TOP ^

Contact us

Contact the NCA (/contact-us)

Suspicious activity reports (SARs) (https://www.ukciu.gov.uk/saronline.aspx)

Verify an NCA officer (https://www.nationalcrimeagency.gov.uk/contact-us/verify-an-nca-officer)

Complaints (https://www.nationalcrimeagency.gov.uk/contact-us/complaints)

CLICK CEOP Advice Help Report (https://www.ceop.police.uk)

0370 496 7622

NCA general enquiries or to verify an NCA officer, available 24/7

(https://www.facebook.com/nca) (https://twitter.com/NCA_UK) (https://www.youtube.com/user/NationalCrimeAgency)

© Crown Copyright

PH-632

Extractive Industries
Transparency Initiative

THE EITI STANDARD 2019

The global standard for the good governance of oil, gas and mineral resources

17 JUNE 2019

PH-633

Complete EITI Standard publication, containing chapter one – Implementation of the EITI Standard and chapter two – Governance and management.

Abridged EITI Standard, containing chapter one – Implementation of the EITI Standard.

EITI website containing complete EITI Standard, guidance notes and examples.

eiti.org/guide

The EITI Standard 2019
Edition 1, 17 June 2019
This edition of the EITI Standard has been produced for the 2019 Global Conference. A second edition will be issued later in 2019 with the Articles of Association as approved at the 17 June Members Meeting.

EITI International Secretariat

This publication (excluding the logo) may be reproduced free of charge in any format or medium provided that it is reproduced accurately and not used in a misleading context.

The material must be acknowledged as EITI copyright with the title and source of the publication specified.

Copyright in the typographical arrangement and design rests with the EITI.

Design by Sue MacDonald.
Printed in Paris, June 2019.

EITI International Secretariat
Rådhusgata 26 0151 Oslo Norway
Tel: +47 222 00 800 Website: www.eiti.org E-mail: secretariat@eiti.org

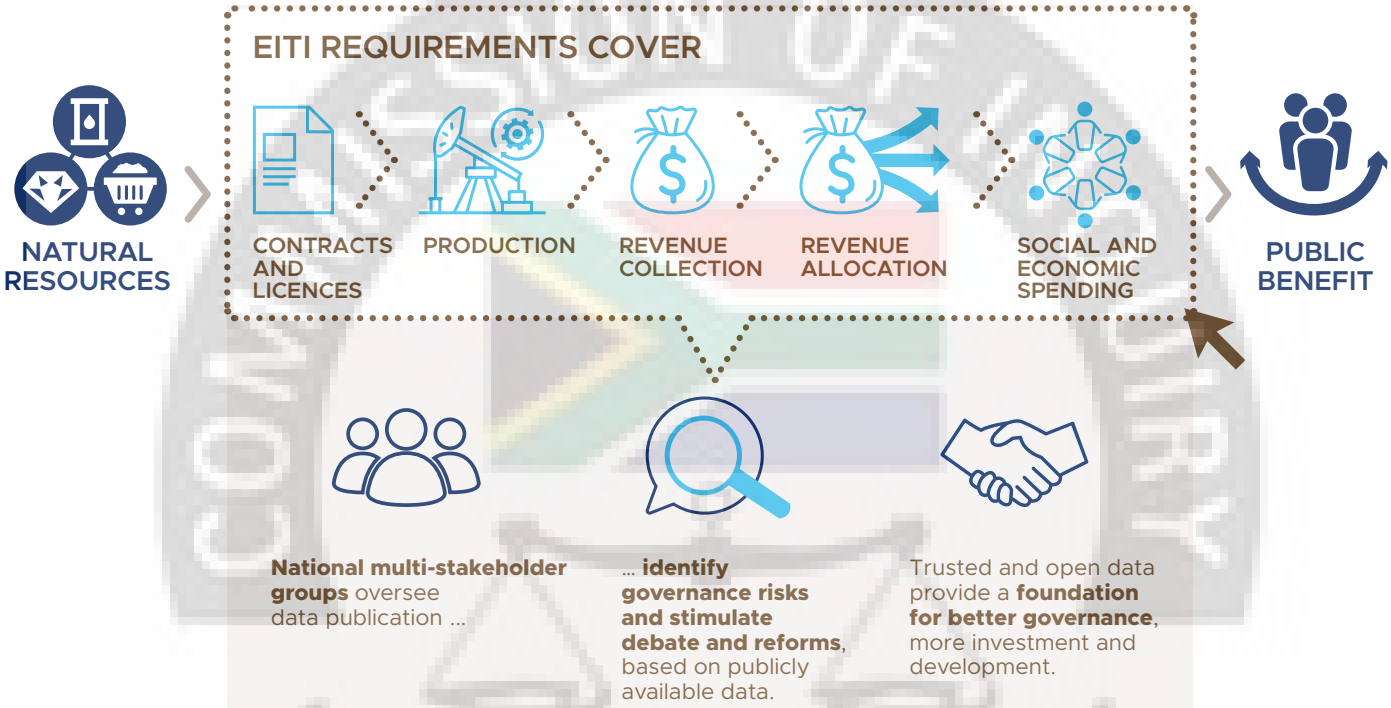
PH-634

THE EITI STANDARD 2019

The global standard for the good governance of oil, gas and mineral resources

COMMISSION OF INQUIRY INTO STATE CAPTURE

HOW THE EITI WORKS
AND HOW IT ACHIEVES IMPACT



PH-636

Contents

Foreword 4

Introduction 5

CHAPTER I: IMPLEMENTATION OF THE EITI STANDARD 6

1. The EITI Principles 6
2. Becoming an EITI implementing country 7
3. Requirements for EITI implementing countries 9
   1. Oversight by the multi-stakeholder group 10
   2. Legal and institutional framework, including allocation of contracts and licenses 15
   3. Exploration and production 21
   4. Revenue collection 22
   5. Revenue allocations 27
   6. Social and economic spending 29
   7. Outcomes and impact 31
4. EITI Board oversight of EITI implementation 34
5. Overview of Validation 41
6. Protocol: Participation of civil society 44
7. Expectations for EITI supporting companies 48
8. Open data policy 49

CHAPTER II: GOVERNANCE AND MANAGEMENT 52

9. Articles of Association 53
10. EITI Openness policy 63
11. EITI Constituency guidelines 64
12. EITI Association code of conduct 65

PH-637

Foreword

Ensuring good governance of the extractive industries is essential for meeting the Sustainable Development Goals and tackling corruption. In the past decade almost USD 2.5 trillion from the extractive industries have been disclosed by EITI countries. But more work remains to be done, especially at a time when trust in governments, multilateralism, even the value of dialogue itself, is under strain.

The EITI Standard has continuously evolved since it was first agreed in 2013. In that time, it has been shaped by the 50 plus countries that implement it, building on emerging practices at the country level. It sets the global standard for transparency and accountability in the extractive industries and has become the model for multi-stakeholder transparency initiatives working in other sectors. It puts into action the EITI Principles, chief of which is a belief shared by all our stakeholders that a country's natural resource wealth should benefit all its citizens. This edition includes for the first time a set of expectations for companies supporting the EITI that contribute to that goal.

The key shift is that the Standard now starts from the assumption that countries and companies should systematically disclose the information through their own systems. New ground has also been broken with disclosures requirements on environmental, social and gender impacts. On the fiscal and legal side, contract transparency will be required for new contracts from 2021 forward, new commodity sales data is being released and reporting is now done at the project level. Much credit is due to the EITI Board, implementing countries and the EITI International Secretariat for pushing for consensus on a range of new requirements that will continue to make the EITI Standard a useful tool for reform.

The EITI and its supporters must respond efficiently and effective to the public interest in extractive sector revenues and governance. My tenure as Chair has seen the rapid change in the world and the landscape for extractive industry transparency. The perceived lack of progress in tackling corruption, tax evasion and illicit financial flows has contributed to the rise of populism and economic nationalism. Transparent and strong institutions that foster good governance remain the best bulwark and remedy against this rising tide.

Fredrik Reinfeldt, Chair of the EITI Board 2016-2019
17 June 2019

Introduction

This EITI Standard consists of two chapters: chapter one, *Implementation of the EITI Standard*; and chapter two, *Governance and management*.

Chapter one, *Implementation of the EITI Standard*, includes:

- **The EITI Principles**, which were agreed by all stakeholders in 2003. These Principles lay out the general aims and commitments by all stakeholders.
- **The EITI Requirements**, which must be adhered to by countries implementing the EITI.
- A section on **EITI Board oversight of EITI implementation**, which outlines the time frames that implementing countries must adhere to and the consequences of non-compliance with the EITI Requirements.
- **Overview of Validation.** Validation provides stakeholders with an impartial assessment of progress in EITI implementation towards meeting the requirements of the EITI Standard.
- **The protocol "Participation of civil society",** which sets out requirements and expectations regarding civil society participation in EITI implementation.
- **Expectations for EITI supporting companies**.
- **The Open data policy**.

Guidance on part one of the EITI Standard is available on eiti.org/guide.

Chapter two addresses the EITI's *Governance and management*. It includes: the **Articles of Association**, which address how the EITI Members' Association is governed and the **EITI Openness policy**, which addresses how the EITI itself should be transparent. Each constituency of the Association has agreed **Constituency guidelines**. It also includes the **EITI Association code of conduct** which establishes expectations for conduct for all EITI Board Members, their alternates, Members of the EITI Association, national and international secretariat staff and members of multi-stakeholder groups.

PH-639

CHAPTER I
Implementation of the EITI Standard

1. The EITI Principles

A diverse group of countries, companies and civil society organisations attended the Lancaster House Conference in London (2003) hosted by the Government of the United Kingdom. They agreed a Statement of Principles to increase transparency over payments and revenues in the extractive sector. These became known as the EITI Principles and are the cornerstone of the EITI.

Box 1 – EITI Principles

1 We share a belief that the prudent use of natural resource wealth should be an important engine for sustainable economic growth that contributes to sustainable development and poverty reduction, but if not managed properly, can create negative economic and social impacts.

2 We affirm that management of natural resource wealth for the benefit of a country's citizens is in the domain of sovereign governments to be exercised in the interests of their national development.

3 We recognise that the benefits of resource extraction occur as revenue streams over many years and can be highly price dependent.

4 We recognise that a public understanding of government revenues and expenditure over time could help public debate and inform choice of appropriate and realistic options for sustainable development.

5 We underline the importance of transparency by governments and companies in the extractive industries and the need to enhance public financial management and accountability.

6 We recognise that achievement of greater transparency must be set in the context of respect for contracts and laws.

7 We recognise the enhanced environment for domestic and foreign direct investment that financial transparency may bring.

8 We believe in the principle and practice of accountability by government to all citizens for the stewardship of revenue streams and public expenditure.

9 We are committed to encouraging high standards of transparency and accountability in public life, government operations and in business.

10 We believe that a broadly consistent and workable approach to the disclosure of payments and revenues is required, which is simple to undertake and to use.

11 We believe that payments' disclosure in a given country should involve all extractive industry companies operating in that country.

12 In seeking solutions, we believe that all stakeholders have important and relevant contributions to make - including governments and their agencies, extractive industry companies, service companies, multilateral organisations, financial organisations, investors and non-governmental organisations.

PH-640

2. Becoming an EITI implementing country

A country intending to implement the EITI is required to undertake a number of steps before applying to become an EITI country. These steps relate to government commitment (1.1), company engagement (1.2), civil society engagement (1.3), the establishment of a multi-stakeholder group (1.4) and agreement on an EITI work plan (1.5). The detailed provisions are set out on pages 10-14. When the country has completed these steps and wishes to be recognised as an EITI implementing country, the government should submit an EITI Application to the EITI Board (see box 2).

Box 2 – How to become an EITI implementing country

When the country has completed the sign-up steps and wishes to be recognised as an EITI implementing country, the government should submit an EITI Application, endorsed by the multi-stakeholder group.[1] The application should describe the activities undertaken to date and provide evidence demonstrating that each of the sign-up steps have been completed. The application should include contact details for government, civil society and private sector stakeholders involved in the EITI.

Once submitted, the application will be made publicly available on the EITI website. The EITI Board will review the application and assess whether the sign-up steps have been completed. The International Secretariat will work closely with the senior individual appointed by the government to lead on EITI implementation in order to clarify any outstanding issues. Based on this and any other available information, the EITI Board's Outreach and Candidature Committee will make a recommendation, within a reasonable time period, to the EITI Board on whether a country's application should be accepted. The EITI Board will make the final decision.

The EITI Board aims to process applications within eight weeks of receiving the application. The EITI Board prefers to make decisions on admitting an EITI country during EITI Board meetings, although may consider taking a decision via Board circular between meetings where appropriate.

When the EITI Board admits an EITI implementing country, it will also establish deadlines for publishing the first EITI Report and undertaking Validation. An implementing country's first EITI disclosures must be made available within 18 months from the date that the country was admitted. Validation will commence within two and a half years of becoming an EITI implementing country. Further information on reporting and Validation deadlines – and the scope for extensions of these deadlines – is outlined in section 4 on EITI Board oversight of EITI implementation.

CONTINUED

1 A standardised application form is available from the International Secretariat.

PH-641

2. Becoming an EITI implementing country CONTINUED

Countries preparing to join the EITI are encouraged to identify potential barriers to systematic disclosures from the outset, for instance by conducting a systematic disclosure feasibility study or addressing opportunities for systematic disclosures as part of the preparations for becoming an EITI implementing country.

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-642

3. Requirements for EITI implementing countries

This section sets out the requirements that must be adhered to by countries implementing the EITI.

The EITI Requirements are minimum requirements and implementing countries are encouraged to go beyond them where stakeholders agree that this is appropriate. Stakeholders are encouraged to consult additional guidance materials on how to best ensure that the requirements are met, available at eiti.org/guide.

Terminology

The use of the terms **'must'**, **'should'** and **'required'** in the EITI Standard indicates that something is **mandatory** and will be taken into account in the assessment of compliance with the EITI Standard.

The use of the term **'expected'** in the EITI Standard indicates that the multi-stakeholder group should **consider the issue** and document their discussions, rationale for disclosure/non-disclosure and any barriers to disclosure. Validation will consider and document the discussions by the multi-stakeholder group.

The use of the terms **'recommended'**, **'encouraged'**, **'may wish'** and **'could'** in the EITI Standard indicates that something is **optional**. Efforts by the multi-stakeholder group will be documented in Validation but will not be taken into account in the overall assessment of compliance with the EITI Standard.

The terms **'systematic disclosure'** and **'mainstreaming'** are used interchangeably. They refer to the desired end-state, where the EITI's disclosure requirements are met through **routine and publicly available company and government reporting.** This could include public financial reporting, annual reports, information portals and other open data initiatives. Systematic disclosure is the expectation, with EITI Reports used to provide additional context, collate the sources where systematic disclosures can be found, and address any gaps and concerns about data quality. EITI disclosure requirements can be met by referencing publicly available information and/or data collected as part of EITI implementation.

PH-643

REQUIREMENT 1

Oversight by the multi-stakeholder group.

OVERVIEW: The EITI requires effective multi-stakeholder oversight, including a functioning multi-stakeholder group that involves the government, companies, and the full, independent, active and effective participation of civil society. The key requirements related to multi-stakeholder oversight include: (1.1) government commitment; (1.2) company engagement; (1.3) civil society engagement; (1.4) the establishment and functioning of a multi-stakeholder group; and (1.5) an agreed work plan with clear objectives for EITI implementation and a timetable that is aligned with the deadlines established by the EITI Board.

1.1 Government commitment.

a) The government is required to issue an unequivocal public statement of its intention to implement the EITI. The statement must be made by the head of state or government, or an appropriately delegated government representative.

b) The government is required to appoint a senior individual to lead the implementation of the EITI. The appointee should have the confidence of all stakeholders, the authority and freedom to coordinate action on the EITI across relevant ministries and agencies, and be able to mobilise resources for EITI implementation.

c) The government must be fully, actively and effectively engaged in the EITI process.

d) The government must ensure that senior government officials are represented in the multi-stakeholder group.

1.2 Company engagement.

a) Companies must be fully, actively and effectively engaged in the EITI process.

b) The government must ensure that there is an enabling environment for company participation with regard to relevant laws, regulations and administrative rules as well as actual practice in implementation of the EITI. The fundamental rights of company representatives substantively engaged in the EITI, including but not restricted to members of the multi-stakeholder group, must be respected.

c) The government must ensure that there are no obstacles to company participation in the EITI process.

REQUIREMENT 1 CONTINUED

1.3 Civil society engagement.

In accordance with the civil society protocol:[2]

a) Civil society must be fully, actively and effectively engaged in the EITI process.

b) The government must ensure that there is an enabling environment for civil society participation with regard to relevant laws, regulations and administrative rules as well as actual practice in implementation of the EITI. The fundamental rights of civil society substantively engaged in the EITI, including but not restricted to members of the multi-stakeholder group, must be respected.

c) The government must ensure that there are no obstacles to civil society participation in the EITI process.

d) The government must refrain from actions which result in narrowing or restricting public debate in relation to implementation of the EITI.

e) Stakeholders, including but not limited to members of the multi-stakeholder group, must:

   i. Be able to speak freely on transparency and natural resource governance issues.

   ii. Be substantially engaged in the design, implementation, monitoring and evaluation of the EITI process, and ensure that it contributes to public debate.

   iii. Have the right to communicate and cooperate with each other.

   iv. Be able to operate freely and express opinions about the EITI without restraint, coercion or reprisal.

1.4 Multi-stakeholder group.

a) The government is required to commit to work with civil society and companies, and establish a multi-stakeholder group to oversee the implementation of the EITI. In establishing the multi-stakeholder group, the government must:

   i. Ensure that the invitation to participate in the group is open and transparent.

   ii. Ensure that stakeholders are adequately represented. This does not mean that they need to be equally represented numerically. The multi-stakeholder group must comprise appropriate stakeholders, including but not necessarily limited to: the private sector; civil society, including independent civil society groups and other civil society such as the media and unions; and relevant government entities, which can also include parliamentarians. Each stakeholder group must have the right to appoint its own representatives, bearing in mind the desirability

2 The civil society protocol is contained in **section 6** of the EITI Standard.

PH-645

REQUIREMENT 1.4 CONTINUED

of pluralistic and diverse representation. The nomination process must be independent and free from any suggestion of coercion. Civil society groups involved in the EITI as members of the multi-stakeholder group must be operationally, and in policy terms, independent of government and/or companies. The multi-stakeholder group and each constituency should consider gender balance in their representation to progress towards gender parity.

iii. Consider establishing the legal basis of the group.

b) The multi-stakeholder group is required to agree clear public Terms of Reference (ToRs) for its work. The ToRs should, at a minimum, include provisions on:

The role, responsibilities and rights of the multi-stakeholder group:

i. Members of the multi-stakeholder group should have the capacity to carry out their duties.

ii. The multi-stakeholder group should undertake effective outreach activities with civil society groups and companies, including through communication such as media, websites and letters, informing stakeholders of the government's commitment to implement the EITI, and the central role of companies and civil society. The multi-stakeholder group should also widely disseminate the public information that results from the EITI process.

iii. Members of the multi-stakeholder group should liaise with their constituency groups.

iv. Members of the multi-stakeholder group are expected to abide by the EITI Association code of conduct.

Approval of work plans and oversight of implementation:

v. The multi-stakeholder group is required to approve annual work plans in accordance with Requirement 1.5.

vi. The multi-stakeholder group should oversee the EITI reporting process and engage in Validation.

Internal governance rules and procedures:

vii. The EITI requires an inclusive decision-making process throughout implementation, with each constituency being treated as a partner. Any member of the multi-stakeholder group has the right to table an issue for discussion. The multi-stakeholder group should agree and publish its procedures for nominating and changing multi-stakeholder group representatives, decision-making, the duration of the mandate and the frequency of meetings. This should include ensuring that there is a process for changing group members that respects the principles set out in Requirement 1.4(a). Where the multi-stakeholder group has a practice of per diems for attending EITI meetings, or other payments to its members, this practice should be transparent and should not create conflicts of interest.

REQUIREMENT 1.4 CONTINUED

viii. There should be sufficient advance notice of meetings and timely circulation of documents prior to their debate and proposed adoption.

ix. The multi-stakeholder group must keep written records of its discussions and decisions.

1.5 Work plan.

The multi-stakeholder group is required to maintain a current work plan which is fully costed and aligned with the reporting and Validation deadlines established by the EITI Board. The work plan must:

a) Set EITI implementation objectives that are linked to the EITI Principles and reflect national priorities for the extractive industries. The multi-stakeholder group should address the steps needed to mainstream EITI implementation in company and government systems. Multi-stakeholder groups are encouraged to explore innovative approaches to extending EITI implementation to inform public debate about natural resource governance and encourage high standards of transparency and accountability in public life, government operations and in business.

b) Reflect the results of consultations with key stakeholders and be endorsed by the multi-stakeholder group.

c) Include measurable and time bound activities to achieve the agreed objectives. The scope of EITI implementation should be tailored to contribute to the desired objectives that have been identified during the consultation process. The work plan must:

i. Assess and outline plans to address any potential capacity constraints in government agencies, companies and civil society that may be an obstacle to effective EITI implementation.

ii. Address the scope of EITI implementation, including plans for strengthening systematic disclosures and addressing technical aspects of reporting, such as comprehensiveness and data reliability (4.1 and 4.9).

iii. Identify and outline plans to address any potential legal or regulatory obstacles to EITI implementation, including, if applicable, any plans to incorporate the EITI Requirements within national legislation or regulation.

iv. Outline the multi-stakeholder group's plans for implementing the recommendations from EITI implementation and Validation.

v. Outline plans for disclosing contracts in accordance with Requirement 2.4(b) and beneficial ownership information in accordance with Requirement 2.5(c)-(f), including milestones and deadlines.

d) Identify domestic and external sources of funding and technical assistance where appropriate in order to ensure timely implementation of the agreed work plan.

PH-647

3. Requirements for EITI implementing countries CONTINUED

REQUIREMENT 1.5 CONTINUED

e) Be made widely available to the public, for example published on the national EITI website and/or other relevant ministry and agency websites, in print media or in places that are easily accessible to the public.

f) Be reviewed and updated annually. In reviewing the work plan, the multi-stakeholder group should consider extending the detail and scope of EITI implementation. In accordance with Requirement 1.4 (b), the multi-stakeholder group is required to document its discussions and decisions.

g) Include a timetable for implementation that is aligned with the deadlines established by the EITI Board (section 4 - EITI Board oversight of EITI implementation) and that takes into account administrative requirements such as procurement processes and funding.

COMMISSION OF INQUIRY INTO STATE CAPTURE

REQUIREMENT 2

Legal and institutional framework, including allocation of contracts and licenses.

OVERVIEW: The EITI requires disclosures on how the extractive sector is managed, enabling stakeholders to understand the laws and procedures for the award of exploration and production rights, the legal, regulatory and contractual frameworks that apply to the extractive sector, and the institutional responsibilities of the State in managing the sector. The EITI Requirements related to a transparent legal framework and awarding of extractive industry rights include: (2.1) legal framework and fiscal regime; (2.2) contract and license allocations; (2.3) register of licenses; (2.4) contracts; (2.5) beneficial ownership; and (2.6) state participation in the extractive sector.

2.1 Legal framework and fiscal regime.

a) Implementing countries must disclose a description of the legal framework and fiscal regime governing the extractive industries. This information must include a summary description of the fiscal regime, including the level of fiscal devolution, an overview of the relevant laws and regulations, a description of the different types of contracts and licenses that govern the exploration and exploitation of oil, gas and minerals, and information on the roles and responsibilities of the relevant government agencies.

b) Where the government is undertaking reforms, the multi-stakeholder group is encouraged to ensure that these are documented.

2.2 Contract and license allocations.

a) Implementing countries are required to disclose the following information related to all contract and license awards and transfers taking place during the accounting period covered by the most recent EITI disclosures, including for companies whose payments fall below the agreed materiality threshold:

   i. A description of the process for transferring or awarding the license;

   ii. The technical and financial criteria used;

   iii. Information about the recipient(s) of the license that has been transferred or awarded, including consortium members where applicable; and

   iv. Any material deviations from the applicable legal and regulatory framework governing license transfers and awards.

   In cases where governments can select different methods for awarding a contract or license (e.g. competitive bidding or direct negotiations), the description of the process for awarding or transferring a license could include an explanation of the rules that determine which procedure should be used and why a particular procedure was selected.

PH-649

REQUIREMENT 2.2 a) CONTINUED

Where there are gaps in the publicly available information, these should be clearly identified. Any significant legal or practical barriers preventing comprehensive disclosure of the information set out above should be documented and explained, including an account of government plans to overcome such barriers and the anticipated timescale for achieving them.

b) Where companies hold licenses that were allocated prior to the period covered by EITI implementation, implementing countries are encouraged to disclose the information set out in 2.2(a).

c) Where licenses are awarded through a bidding process, the government is required to disclose the list of applicants and the bid criteria.

d) The multi-stakeholder group may wish to include additional information on the allocation of licenses as part of the EITI disclosures. This could include commentary on the efficiency and effectiveness of licensing procedures, and a description of procedures, actual practices and grounds for renewing, suspending or revoking a contract or license.

2.3 Register of licenses.

a) The term 'license' in this context refers to any license, lease, title, permit, contract or concession by which the government confers on a company(ies) or individual(s) rights to explore or exploit oil, gas and/or mineral resources.

b) Implementing countries are required to maintain a publicly available register or cadastre system(s) with the following timely and comprehensive information regarding each of the licenses pertaining to companies within the agreed scope of EITI implementation:

i. License holder(s).

ii. Where collated, coordinates of the license area. Where coordinates are not collated, the government is required to ensure that the size and location of the license area are disclosed in the license register and that the coordinates are publicly available from the relevant government agency without unreasonable fees and restrictions. The disclosures should include guidance on how to access the coordinates and the cost, if any, of accessing the data. The government should also document plans and timelines for making this information freely and electronically available through the license register.

iii. Date of application, date of award and duration of the license.

iv. In the case of production licenses, the commodity being produced.

It is expected that the license register or cadastre includes information about licenses held by all entities, including companies and individuals or groups that are outside the agreed scope of EITI implementation, i.e. where their payments fall below the agreed materiality threshold. Any significant legal or practical barriers preventing such comprehensive disclosure should be documented and explained, including an account of government plans for seeking to overcome such barriers and the anticipated timescale for achieving them.

REQUIREMENT 2.3 CONTINUED

c) Where such registers or cadastres do not exist or are incomplete, any gaps in the publicly available information should be disclosed and efforts to strengthen these systems documented.

2.4 Contracts.

a) Implementing countries are required to disclose any contracts and licenses that are granted, entered into or amended from 1 January 2021. Implementing countries are encouraged to publicly disclose any contracts and licenses that provide the terms attached to the exploitation of oil, gas and minerals.

b) The multi-stakeholder group is expected to agree and publish a plan for disclosing contracts with a clear time frame for implementation and addressing any barriers to comprehensive disclosure. This plan will be integrated into work plans covering 2020 onwards.

c) It is a requirement to document the government's policy on disclosure of contracts and licenses that govern the exploration and exploitation of oil, gas and minerals. This should include:

   i. A description of whether legislation or government policy addresses the issue of disclosure of contracts and licenses, including whether it requires or prohibits disclosure of contracts and licenses. If there is no existing legislation, an explanation of where the government policy is embodied should be included, and the multi-stakeholder group should document its discussion on what constitutes government policy on contract disclosures. Any reforms relevant to the disclosure of contracts and licenses planned or underway should be documented.

   ii. An overview of which contracts and licenses are publicly available. Implementing countries should provide a list of all active contracts and licenses, indicating which are publicly available and which are not. For all published contracts and licenses, it should include a reference or link to the location where the contract or license is published. If a contract or license is not published, the legal or practical barriers should be documented and explained.

   iii. Where disclosure practice deviates from legislative or government policy requirements concerning the disclosure of contracts and licenses, an explanation for the deviation should be provided.

d) The term 'contract' in 2.4(a) means:

   i. The full text of any contract, concession, production-sharing agreement or other agreement granted by, or entered into by, the government which provides the terms attached to the exploitation of oil, gas and mineral resources.

PH-651

REQUIREMENT 2.4 d) CONTINUED

ii. The full text of any annex, addendum or rider which establishes details relevant to the exploitation rights described in 2.4(d)(i) or the execution thereof.

iii. The full text of any alteration or amendment to the documents described in 2.4(d)(i) and 2.4(d)(ii).

e) The term 'license' in 2.4(a) means:

i. The full text of any license, lease, title or permit by which a government confers on a company(ies) or individual(s) rights to exploit oil, gas and/or mineral resources.

ii. The full text of any annex, addendum or rider that establishes details relevant to the exploitation rights described in in 2.4(e)(i) or the execution thereof.

iii. The full text of any alteration or amendment to the documents described in 2.4(e)(i) and 2.4(e)(ii).

2.5 Beneficial ownership.

a) It is recommended that implementing countries maintain a publicly available register of the beneficial owners of the corporate entity(ies) that apply for or hold a participating interest in an exploration or production oil, gas or mining license or contract, including the identity(ies) of their beneficial owner(s), the level of ownership and details about how ownership or control is exerted. Where possible, beneficial ownership information should be incorporated in existing filings by companies to corporate regulators, stock exchanges or agencies regulating extractive industry licensing. Where this information is already publicly available, the EITI Report should include guidance on how to access this information.

b) Implementing countries are required to document the government's policy and multi-stakeholder group's discussion on disclosure of beneficial ownership. This should include details of the relevant legal provisions, actual disclosure practices and any reforms that are planned or underway related to beneficial ownership disclosure.

c) As of 1 January 2020, it is required that implementing countries request, and companies publicly disclose, beneficial ownership information. This applies to corporate entity(ies) that apply for or hold a participating interest in an exploration or production oil, gas or mining license or contract and should include the identity(ies) of their beneficial owner(s), the level of ownership and details about how ownership or control is exerted. Any significant gaps or weaknesses in reporting on beneficial ownership information must be disclosed, including naming any entities that failed to submit all or parts of the beneficial ownership information. Where a country is facing constitutional or significant practical barriers to the implementation of this requirement by 1 January 2020, the country may seek adapted implementation in accordance with Article 1 of the EITI Board's procedures for oversight of EITI implementation in section 4.

REQUIREMENT 2.5 CONTINUED

d) Information about the identity of the beneficial owner should include the name of the beneficial owner, their nationality, and their country of residence, as well as identifying any politically exposed persons. It is also recommended that their national identity number, date of birth, residential or service address, and means of contact are disclosed.

e) The multi-stakeholder group should assess any existing mechanisms for assuring the reliability of beneficial ownership information and agree an approach for corporate entities within the scope of 2.5(c) to assure the accuracy of the beneficial ownership information they provide. This could include requiring companies to attest the beneficial ownership declaration form through sign-off by a member of the senior management team or senior legal counsel, or submit supporting documentation.

f) Definition of beneficial ownership:

   i. A beneficial owner in respect of a company means the natural person(s) who directly or indirectly ultimately owns or controls the corporate entity.

   ii. The multi-stakeholder group should agree an appropriate definition of the term 'beneficial owner'. The definition should be aligned with (f)(i) above and take international norms and relevant national laws into account, and should include ownership threshold(s). The definition should also specify reporting obligations for politically exposed persons.

   iii. Publicly listed companies, including wholly-owned subsidiaries, are required to disclose the name of the stock exchange and include a link to the stock exchange filings where they are listed to facilitate public access to their beneficial ownership information.

   iv. In the case of joint ventures, each entity within the venture should disclose its beneficial owner(s), unless it is publicly listed or is a wholly-owned subsidiary of a publicly listed company. Each entity is responsible for the accuracy of the information provided.

g) Implementing countries and multi-stakeholder groups should also address disclosure of legal owners and share of ownership.

2.6 State participation.

a) Where state participation in the extractive industries gives rise to material revenue payments, implementing countries must disclose:

   i. An explanation of the role of state-owned enterprises (SOEs) in the sector and prevailing rules and practices regarding the financial relationship between the government and SOEs, i.e. the rules and practices governing transfers of funds between the SOE(s) and the state, retained earnings, reinvestment and third-party financing. This should include disclosures of transfers, retained earnings, reinvestment and third-party financing related to SOE joint ventures and subsidiaries.

PH-653

3. Requirements for EITI implementing countries CONTINUED

REQUIREMENT 2.6 a) i. CONTINUED

For the purpose of EITI implementation, a state-owned enterprise (SOE) is a wholly or majority government-owned company that is engaged in extractive activities on behalf of the government. Based on this, the multi-stakeholder group is encouraged to discuss and document its definition of SOEs, taking into account national laws and government structures.

ii. Disclosures from the government and SOE(s) of their level of ownership in mining, oil and gas companies operating within the country's oil, gas and mining sector, including those held by SOE subsidiaries and joint ventures, and any changes in the level of ownership during the reporting period.

This information should include details regarding the terms attached to their equity stake, including their level of responsibility for covering expenses at various phases of the project cycle, e.g. full-paid equity, free equity or carried interest. Where there have been changes in the level of government and SOE(s) ownership during the EITI reporting period, the government and SOE(s) are expected to disclose the terms of the transaction, including details regarding valuation and revenues. Where the government and SOE(s) have provided loans or loan guarantees to mining, oil and gas companies operating within the country, details on these transactions should be disclosed, including loan tenor and terms (i.e. repayment schedule and interest rate). Multi-stakeholder groups may wish to consider comparing loans terms with commercial lending terms.

b) SOEs are expected to publicly disclose their audited financial statements, or the main financial items (i.e. balance sheet, profit/loss statement, cash flows) where financial statements are not available.

c) Implementing countries are encouraged to describe the rules and practices related to SOEs' operating and capital expenditures, procurement, subcontracting and corporate governance, e.g. composition and appointment of the Board of Directors, Board's mandate and code of conduct.

REQUIREMENT 3

Exploration and production.

OVERVIEW: The EITI requires disclosures of information related to exploration and production, enabling stakeholders to understand the potential of the sector. The EITI Requirements related to a transparency in exploration and production activities include: (3.1) information about exploration activities; (3.2) production data; and (3.3) export data.

3.1 Exploration.

Implementing countries should disclose an overview of the extractive industries, including any significant exploration activities.

3.2 Production.

Implementing countries must disclose timely production data, including production volumes and values by commodity. This data could be further disaggregated by region, company or project, and include sources and the methods for calculating production volumes and values.

3.3 Exports.

Implementing countries must disclose timely export data, including export volumes and the value by commodity. This data could be further disaggregated by region, company or project, and include sources and the methods for calculating export volumes and values.

PH-655

REQUIREMENT 4

Revenue collection.

OVERVIEW: An understanding of company payments and government revenues can inform public debate about the governance of the extractive industries. The EITI requires comprehensive disclosure of company payments and government revenues from the extractive industries. The EITI Requirements related to revenue collection include: (4.1) comprehensive disclosure of taxes and revenues; (4.2) sale of the state's share of production or other revenues collected in kind; (4.3) infrastructure provisions and barter arrangements; (4.4) transportation revenues; (4.5) SOE transactions; (4.6) subnational payments; (4.7) level of disaggregation; (4.8) data timeliness; and (4.9) data quality of the disclosures.

4.1 Comprehensive disclosure of taxes and revenues.

a) The EITI requires disclosure of all material payments by oil, gas and mining companies to governments ("payments") and all material revenues received by governments from oil, gas and mining companies ("revenues") to a wide audience in a publicly accessible, comprehensive and comprehensible manner. The expectation is that implementing countries will disclose the requisite information through routine government and corporate reporting (websites, annual reports, etc.), with EITI Reports used to collate this information and address any concerns about gaps and data quality.

b) The multi-stakeholder group is required to agree which payments and revenues are material and therefore must be disclosed, including appropriate materiality definitions and thresholds. Payments and revenues are considered material if their omission or misstatement could significantly affect the comprehensiveness of the disclosures. A description of each revenue stream, related materiality definitions and thresholds should be disclosed. In establishing materiality definitions and thresholds, the multi-stakeholder group should consider the size of the revenue streams relative to total revenues. The multi-stakeholder group should document the options considered and the rationale for establishing the definitions and thresholds.

c) The following revenue streams should be included:

   i. The host government's production entitlement (such as profit oil)

   ii. National state-owned company production entitlement

   iii. Profits taxes

   iv. Royalties

   v. Dividends

   vi. Bonuses, such as signature, discovery and production bonuses

   vii. Licence fees, rental fees, entry fees and other considerations for licences and/or concessions

REQUIREMENT 4.1 c) CONTINUED

viii. Any other significant payments and material benefit to government

Any revenue streams or benefits should only be excluded where they are not applicable or where the multi-stakeholder group agrees that their omission will not materially affect the comprehensiveness of the government and company disclosures.

d) Implementing countries must ensure that all government entities receiving material revenues from oil, gas and mining companies are required to comprehensively disclose these revenues in accordance with the agreed scope. Government entities should only be exempted from disclosure if it can be demonstrated that their revenues are not material. Unless there are significant practical barriers, the government is additionally required to provide aggregate information about the amount of total revenues received from each of the benefit streams agreed in the scope of EITI implementation, including revenues that fall below agreed materiality thresholds. Where this data is not available, the Independent Administrator should draw on any relevant data and estimates from other sources in order to provide a comprehensive account of the total government revenues.

All oil, gas and mining companies making material payments to the government are required to comprehensively disclose these payments in accordance with the agreed scope. A company should only be exempted from disclosure if it can be demonstrated that its payments are not material.

e) Companies are expected to publicly disclose their audited financial statements, or the main items (i.e. balance sheet, profit/loss statement, cash flows) where financial statements are not available.

4.2 Sale of the state's share of production or other revenues collected in kind.

a) Where the sale of the state's share of production of oil, gas and/or mineral resources or other revenues collected in kind is material, the government, including state-owned enterprises, are required to disclose the volumes received and sold by the state (or third parties appointed by the state to sell on their behalf), the revenues received from the sale, and the revenues transferred to the state from the proceeds of oil, gas and minerals sold. Where applicable, this should include payments (in cash or in kind) related to swap agreements and resource-backed loans.

The published data must be disaggregated by individual buying company and to levels commensurate with the reporting of other payments and revenue streams (4.7). Multi-stakeholder groups, in consultation with buying companies, are expected to consider whether disclosures should be broken down by individual sale, type of product and price.

The disclosures could include ownership of the product sold and the nature of the contract (e.g. spot or term).

PH-657

REQUIREMENT 4.2 CONTINUED

b) Implementing countries including state-owned enterprises are encouraged to disclose a description of the process for selecting the buying companies, the technical and financial criteria used to make the selection, the list of selected buying companies, any material deviations from the applicable legal and regulatory framework governing the selection of buying companies, and the related sales agreements.

c) Companies buying oil, gas and/or mineral resources from the state, including state-owned enterprises (or third parties appointed by the state to sell on their behalf), are encouraged to disclose volumes received from the state or state-owned enterprise and payments made for the purchase of oil, gas and/or mineral resources. This could include payments (in cash or in kind) related to swap agreements and resource-backed loans.

The published data could be disaggregated by individual seller, contract or sale.

The disclosures could for each sale include information on the nature of the contract (e.g. spot or term) and load port.

d) Where there are concerns related to data reliability and where practically feasible, the multi-stakeholder group should consider further efforts to address any gaps, inconsistencies and irregularities in the information disclosed.

4.3 Infrastructure provisions and barter arrangements.

The multi-stakeholder group is required to consider whether there are any agreements, or sets of agreements involving the provision of goods and services (including loans, grants and infrastructure works), in full or partial exchange for oil, gas or mining exploration or production concessions or physical delivery of such commodities. To be able to do so, the multi-stakeholder group needs to gain a full understanding of: the terms of the relevant agreements and contracts, the parties involved, the resources which have been pledged by the state, the value of the balancing benefit stream (e.g. infrastructure works), and the materiality of these agreements relative to conventional contracts.

Where the multi-stakeholder group concludes that these agreements are material, the multi-stakeholder group is required to ensure that EITI implementation addresses these agreements and disclosures provide a level of detail and disaggregation commensurate with the other payments and revenue streams. The multi-stakeholder group is required to agree a procedure to address data quality and assurance of the information set out above, in accordance with Requirement 4.9.

4.4 Transportation revenues.

Where revenues from the transportation of oil, gas and minerals are material, the government and state-owned enterprises (SOEs) are expected to disclose the revenues received. The published data must provide a level of detail and

REQUIREMENT 4.4 CONTINUED

disaggregation commensurate with other payments and revenue streams (4.7). The multi-stakeholder group is encouraged to agree a procedure to address data quality and assurance of information on transportation revenues, in accordance with Requirement 4.9.

Implementing countries could disclose:

i. A description of the transportation arrangements including: the product; transportation route(s); and the relevant companies and government entities, including SOE(s), involved in transportation.

ii. Definitions of the relevant transportation taxes, tariffs or other relevant payments, and the methodologies used to calculate them.

iii. Disclosure of tariff rates and volume of the transported commodities.

iv. Disclosure of revenues received by government entities and SOE(s), in relation to transportation of oil, gas and minerals.

4.5 Transactions related to state-owned enterprises (SOEs).

The multi-stakeholder group must ensure that the reporting process comprehensively addresses the role of SOEs, including comprehensive and reliable disclosures of material company payments to SOEs, SOE transfers to government agencies and government transfers to SOEs.

4.6 Subnational payments.

It is required that the multi-stakeholder group establishes whether direct payments, within the scope of the agreed benefit streams, from companies to subnational government entities are material. Where material, the multi-stakeholder group is required to ensure that company payments to subnational government entities and the receipt of these payments are disclosed. The multi-stakeholder group is required to agree a procedure to address data quality and assurance of information on subnational payments, in accordance with Requirement 4.9.

4.7 Level of disaggregation.

It is required that EITI data is disaggregated by each individual project, company, government entity and revenue stream.

A project is defined as operational activities that are governed by a single contract, license, lease, concession or similar legal agreement, and form the basis for payment liabilities with a government. Nonetheless, if multiple such agreements are substantially interconnected, the multi-stakeholder group must clearly identify and document which instances are considered a single project.

Substantially interconnected agreements are a set of operationally and geographically integrated contracts, licenses, leases or concessions or related agreements with substantially similar terms that are signed with a government, giving rise to payment liabilities. Such agreements can be governed by a single contract, joint venture, production sharing agreement or other overarching legal agreement.

PH-659

REQUIREMENT 4.7 CONTINUED

Where a payment covered by the scope of EITI disclosures is levied at entity level rather than at project level, the company may disclose the payment at the entity level.

4.8 Data timeliness.

a) Implementing countries are expected to publish regular and timely information in accordance with the EITI Standard and the agreed work plan (1.5) on an annual basis. The multi-stakeholder group should agree the accounting period covered by the EITI disclosures.

b) The data must be no older than the second to last complete accounting period, e.g. information pertaining to the financial year 2018 must be published at the latest by 31 December 2020.

4.9 Data quality and assurance.

a) The EITI requires an assessment of whether the payments and revenues are subject to credible, independent audit, applying international auditing standards. The expectation is that government and company disclosures as per Requirement 4 are subject to credible, independent audit, applying international auditing standards. The expectation is that disclosures as per Requirement 4 will include an explanation of the underlying audit and assurance procedures that the data has been subject to, with public access to the supporting documentation.

b) The multi-stakeholder group is required to agree a procedure to address data quality and assurance based on a standard procedure endorsed by the EITI Board.[3] The multi-stakeholder group is required to apply the standard procedure without any material deviations. Should the multi-stakeholder group wish to deviate from the standard procedures, approval from the EITI Board must be sought in advance. The request from the multi-stakeholder group should address: (i) the rationale for deviating from the standard procedure; (ii) whether there is routine disclosure of the data required by the EITI Standard in requisite detail; (iii) whether the financial data is subject to credible, independent audit, applying international standards, and (iv) whether there is sufficient retention of historical data.

3 Available from the International Secretariat and eiti.org.

REQUIREMENT 5

Revenue allocations.

OVERVIEW: The EITI requires disclosures of information related to revenue allocations, enabling stakeholders to understand how revenues are recorded in the national and, where applicable, subnational budgets, as well as track social expenditures by companies. The EITI Requirements related to revenue allocations include: (5.1) distribution of revenues; (5.2) subnational transfers; and (5.3) revenue management and expenditures.

5.1 Distribution of extractive industry revenues.

Implementing countries must disclose a description of the distribution of revenues from the extractive industries.

a) Implementing countries should indicate which extractive industry revenues, whether cash or in-kind, are recorded in the national budget. Where revenues are not recorded in the national budget, the allocation of these revenues must be explained, with links provided to relevant financial reports as applicable, e.g. sovereign wealth and development funds, sub-national governments, state-owned enterprises and other extra-budgetary entities.

b) Multi-stakeholder groups are encouraged to reference national revenue classification systems and international standards such as the IMF Government Finance Statistics Manual.

5.2 Subnational transfers.

a) Where transfers between national and subnational government entities are related to revenues generated by the extractive industries and are mandated by a national constitution, statute or other revenue sharing mechanism, the multi-stakeholder group is required to ensure that material transfers are disclosed. Implementing countries should disclose the revenue sharing formula, if any, as well as any discrepancies between the transfer amount calculated in accordance with the relevant revenue sharing formula and the actual amount that was transferred between the central government and each relevant subnational entity. The multi-stakeholder group is encouraged to agree a procedure to address data quality and assurance of information on subnational transfers, in accordance with Requirement 4.9. Where there are constitutional or significant practical barriers to the participation of subnational government entities, the multi-stakeholder group may seek adapted implementation in accordance with Article 1 of the EITI Board's procedures for oversight of EITI implementation in section 4.

b) The multi-stakeholder group is encouraged to ensure that any material discretionary or ad-hoc transfers are also disclosed, and agree a procedure to address data quality and assurance of information on such transfers, in accordance with Requirement 4.9.

PH-661

REQUIREMENT 5.2 CONTINUED

c) The multi-stakeholder group may further wish to report on how extractive revenues earmarked for specific programmes or investments at the subnational level are managed, and actual disbursements.

5.3 Revenue management and expenditures.

The multi-stakeholder group is encouraged to disclose further information on revenue management and expenditures, including:

a) A description of any extractive revenues earmarked for specific programmes or geographic regions. This should include a description of the methods for ensuring accountability and efficiency in their use.

b) A description of the country's budget and audit processes and links to the publicly available information on budgeting, expenditures and audit reports.

c) Timely information from the government that will further public understanding and debate around issues of revenue sustainability and resource dependence. This may include the assumptions underpinning forthcoming years in the budget cycle and relating to projected production, commodity prices and revenue forecasts arising from the extractive industries and the proportion of future fiscal revenues expected to come from the extractive sector.

REQUIREMENT 6

Social and economic spending.

OVERVIEW: The EITI encourages disclosures of information related to revenue management and expenditures, helping stakeholders to assess whether the extractive sector is leading to the desirable social and economic and environmental impacts and outcomes. The EITI Requirements related to revenue allocations include: (6.1) social and environmental expenditures by companies; (6.2) SOE quasi-fiscal expenditures; (6.3) an overview of the contribution of the extractive sector to the economy; and (6.4) the environmental impact of extractive activities.

6.1 Social and environmental expenditures by extractive companies.

a) Where material social expenditures by companies are mandated by law or the contract with the government that governs the extractive investment, implementing countries must disclose these transactions. The multi-stakeholder group is required to agree a procedure to address data quality and assurance of information on social and environmental expenditures, in accordance with Requirement 4.9. Where such benefits are provided in kind, it is required that implementing countries disclose the nature and the deemed value of the in-kind transaction. Where the beneficiary of the mandated social expenditure is a third party, i.e. not a government agency, it is required that the name and function of the beneficiary be disclosed. Where reconciliation is not feasible, countries should provide unilateral company and/or government disclosures of these transactions.

b) Where material payments by companies to the government related to the environment are mandated by law, regulation or contract that governs the extractive investment, such payments must be disclosed.

c) Where the multi-stakeholder group agrees that discretionary social and environmental expenditures and transfers are material, the multi-stakeholder group is encouraged to develop a reporting process with a view to achieving transparency commensurate with the disclosure of other payments and revenues. The multi-stakeholder group is encouraged to agree a procedure to address data quality and assurance of the information set out above, in accordance with Requirement 4.9.

6.2 Quasi-fiscal expenditures.

Where state participation in the extractive industries gives rise to material revenue payments, implementing countries must include disclosures from SOEs on their quasi-fiscal expenditures. The multi-stakeholder group is required to develop a reporting process with a view to achieving a level of transparency commensurate with other payments and revenue streams, and should include SOE subsidiaries and joint ventures.

PH-663

REQUIREMENT 6.2 CONTINUED

Quasi-fiscal expenditures include arrangements whereby SOEs undertake public social expenditure such as payments for social services, public infrastructure, fuel subsidies and national debt servicing, etc. outside of the national budgetary process. Implementing countries and multi-stakeholder groups may wish to take the IMF's definition of quasi-fiscal expenditures into account when considering whether expenditures are considered quasi-fiscal.

6.3 The contribution of the extractive sector to the economy.

Implementing countries must disclose, when available, information about the contribution of the extractive industries to the economy for the fiscal year covered by EITI implementation. It is required that this information includes:

a) The size of the extractive industries in absolute terms and as a percentage of GDP as well as an estimate of informal sector activity, including but not necessarily limited to artisanal and small-scale mining.

b) Total government revenues generated by the extractive industries (including taxes, royalties, bonuses, fees and other payments) in absolute terms and as a percentage of total government revenues.

c) Exports from the extractive industries in absolute terms and as a percentage of total exports.

d) Employment in the extractive industries in absolute terms and as a percentage of the total employment. The information should be disaggregated by gender and, when available, further disaggregated by company and occupational level.

e) Key regions/areas where production is concentrated.

6.4 Environmental impact of extractive activities.

Implementing countries are encouraged to disclose information on the management and monitoring of the environmental impact of the extractive industries. This could include:

a) An overview of relevant legal provisions and administrative rules as well as actual practice related to environmental management and monitoring of extractive investments in the country. This could include information on environmental impact assessments, certification schemes, licences and rights granted to oil, gas and mining companies, as well as information on the roles and responsibilities of relevant government agencies in implementing the rules and regulations. It could further include information on any reforms that are planned or underway.

b) Information on regular environmental monitoring procedures, administrative and sanctioning processes of governments, as well as environmental liabilities, environmental rehabilitation and remediation programmes.

REQUIREMENT 7

Outcomes and impact.

OVERVIEW: Regular disclosure of extractive industry data is of little practical use without public awareness, understanding of what the figures mean, and public debate about how resource revenues can be used effectively. The EITI Requirements related to outcomes and impact seek to ensure that stakeholders are engaged in dialogue about natural resource revenue management. EITI disclosures lead to the fulfilment of the EITI Principles by contributing to wider public debate. It is also vital that lessons learnt during implementation are acted upon, that recommendations from EITI implementations are considered and acted on where appropriate and that EITI implementation is on a stable, sustainable footing.

7.1 Public debate.

The multi-stakeholder group must ensure that government and company disclosures comprehensible, actively promoted, publicly accessible and contributes to public debate. Key audiences should include government, parliamentarians, civil society, companies and the media.

a) The multi-stakeholder group is required to:

   i. Ensure that the information is widely accessible and distributed. The multi-stakeholder group is encouraged to break this down into thematic reports and make this available online.

   ii. Ensure that the information is comprehensible, including by ensuring that it is written in a clear, accessible style and in appropriate languages and consider access challenges and information needs of different genders and subgroups of citizens.

   iii. Ensure that outreach events, whether organised by government, civil society or companies, are undertaken to spread awareness of and facilitate dialogue about governance of extractive resources, building on EITI disclosures across the country in a socially inclusive manner.

b) The multi-stakeholder group is encouraged to:

   i. Produce brief summary reports, with clear and balanced analysis of the information, ensuring that the data sources and authorship are clearly stated.

   ii. Summarise and compare the share of each revenue stream to the total amount of revenue that accrues to each respective level of government.

   iii. Undertake capacity-building efforts, especially with civil society and through civil society organisations, to improve understanding of the information and data from the reports and online disclosures and encourage use of the information by citizens, the media and others.

PH-665

REQUIREMENT 7 CONTINUED

7.2 Data accessibility and open data.

Implementing countries should ensure that EITI disclosures are made publicly accessible. The multi-stakeholder group should:

a) Agree a clear open data policy on the access, release and re-use of EITI data. Government agencies and companies are expected to publish EITI data under an open license, and to make users aware that information can be reused without prior consent.

b) Make the data available in an open data format online and publicise its availability. Open data format means that data can be made accessible in CSV or Excel format and could contain all tables, charts and figures from EITI Reports.

c) Complete summary data files for each fiscal year covered by the EITI in accordance with the template approved by the EITI Board.

d) The multi-stakeholder group is encouraged to make systematically disclosed data machine readable and inter-operable, and to code or tag EITI disclosures and other data files so that the information can be compared with other publicly available data.

7.3 Recommendations from EITI implementation.

With a view to strengthening the impact of EITI implementation on natural resource governance, the multi-stakeholder group is required to take steps to act upon lessons learnt; to identify, investigate and address the causes of any information gaps and discrepancies; and to consider the recommendations resulting from EITI implementation. The multi-stakeholder group can consider agreeing recommendations for strengthening government systems and natural resource governance. Where appropriate, implementing countries are encouraged to follow up on such recommendations.

7.4 Review the outcomes and impact of EITI implementation.

The multi-stakeholder group is required to review the outcomes and impact of EITI implementation on natural resource governance.

a) The multi-stakeholder group is required to document their annual review of impact and outcomes of EITI implementation in an annual progress report or through other means agreed by the multi-stakeholder group. This should include any actions undertaken to address issues that the multi-stakeholder group has identified as priorities for EITI implementation.[4] The annual review of impact and outcomes must include:

   i. A summary of EITI activities undertaken in the previous year and an account of the outcomes of these activities.

4 A standard template is available from the International Secretariat.

REQUIREMENT 7.4 a) CONTINUED

ii. An assessment of progress towards meeting each EITI Requirement, and any steps taken to exceed the requirements. This should include any actions undertaken to address issues that the multi-stakeholder group has identified as priorities for EITI implementation.

iii. An overview of the multi-stakeholder group's responses to and progress made in addressing the recommendations from reconciliation and Validation in accordance with Requirement 7.3. The multi-stakeholder group is required to list each recommendation and the corresponding activities that have been undertaken to address the recommendations and the level of progress in implementing each recommendation. Where the government or the multi-stakeholder group has decided not to implement a recommendation, it is required that the multi-stakeholder group documents the rationale.

iv. An assessment of progress towards achieving the objectives set out in its work plan (Requirement 1.5), including the impact and outcomes of the stated objectives.

v. A narrative account of efforts to strengthen the impact of EITI implementation on natural resource governance, including any actions to extend the detail and scope of EITI reporting or to increase engagement with stakeholders.

In addition, the multi-stakeholder group is encouraged to document how it has taken gender considerations and inclusiveness into account.

b) All stakeholders should be able to participate in reviewing the impact of EITI implementation. Civil society groups and industry involved in the EITI, particularly, but not only, those serving on the multi-stakeholder group, should be able to provide feedback on the EITI process and have their views reflected in the annual review of impact and outcomes.

PH-667

4. EITI Board oversight of EITI implementation

This section outlines the procedures and criteria that the EITI Board uses in overseeing and validating EITI implementation. This includes the time frames established by the EITI Board for publication of EITI data and oversight of the Validation process.

Article 1 – Adapted implementation.

Should the multi-stakeholder group conclude that it faces exceptional circumstances that necessitate deviation from the implementation requirements, it must seek prior EITI Board approval for adapted implementation. The request must be endorsed by the multi-stakeholder group and reflected in the work plan. The request should explain the rationale for the adapted implementation.

The EITI Board will only consider allowing adaptations in exceptional circumstances. In considering such requests, the EITI Board will place a priority on the need for comparable treatment between countries and ensuring that the EITI Principles are upheld, including ensuring that the EITI process is sufficiently inclusive, and that EITI disclosures are comprehensive, reliable and will contribute to public debate.

Article 2 – Disclosure and reporting deadlines.

Implementing countries are required to publish timely information (Requirement 4.8). Implementing countries are required to publish the requested information (typically through an EITI Report) within 18 months of being admitted as an EITI country. Thereafter, the published data must be no older than the second to last complete accounting period, e.g. information pertaining to the financial year ending 31 December 2018 must be published at the latest by 31 December 2020.

If the data is not published by the required deadline, the country will be suspended. The suspension will be lifted if the EITI Board is satisfied that the outstanding data is published within six months of the deadline. If the outstanding data is not published within six months of the deadline, the suspension will remain in force until the EITI Board is satisfied that the country has published EITI data in accordance with Requirement 4.8. If the suspension is in effect for more than one year, the EITI Board will delist the country.

Article 3 – Initial Validation deadline.

When the EITI Board admits implementing countries, it will establish a deadline for the commencement of Validation within two and a half years. Subsequent to considering the findings, the Board will establish a deadline for further Validations (Article 5).

Article 4 – EITI Validation process.

a) Assessment of each EITI Requirement

The Validation process will assess the country's progress in complying with each of the EITI Requirements. Detailed guidance on the types of evidence that are required in order to make an assessment on individual requirements is set out in the Validation Guide. The level of progress and compliance with each individual EITI Requirement shall be indicated by applying one of the following designations:

Outstanding progress. In order for the EITI Board to conclude that a country has made outstanding progress, Validation needs to demonstrate that all aspects of the requirement, including 'expected', 'encouraged' and 'recommended' aspects, have been implemented and that the broader objective of the requirement has been fulfilled through systematic disclosures in government and company systems.

Satisfactory progress. In order for the EITI Board to conclude that a country has made satisfactory progress, Validation needs to demonstrate that all aspects of the requirement have been implemented and that the broader objective of the requirement has been fulfilled.

Meaningful progress. In order for the EITI Board to conclude that a country has made meaningful progress, Validation needs to demonstrate that significant aspects of the requirement have been implemented and that the broader objective of the requirement is being fulfilled.

Inadequate progress. In order for the EITI Board to conclude that a country has made inadequate progress, Validation needs to demonstrate that significant aspects of the requirement have not been implemented and that the broader objective of the requirement is far from fulfilled.

No progress. In order for the EITI Board to conclude that a country has made no progress, Validation needs to demonstrate that all or nearly all aspects of the requirement have not been implemented, and that the broader objective of the requirement is not fulfilled.

b) Overall assessments

The EITI Board will make an assessment of overall compliance with all requirements in the EITI Standard. In determining a country's overall assessment, the EITI Board will apply the same scale as used for the assessment of the individual requirements outlined in Article 4(a) above. The Board will take into account the following factors:

- The results of the assessment of the individual requirements and whether these results all taken together clearly point to an overall assessment of 'satisfactory progress', 'meaningful progress', 'inadequate progress', or 'no progress';
- The advice and recommendations of Validators and the Validation Committee;

PH-669

ARTICLE 4 b) CONTINUED

- The nature of the requirements that have not been implemented and how close the requirements are to being met;
- The magnitude and complexity of the extractive sector of the country;
- Other barriers to meeting requirements such, as but not limited to, state fragility and recent or ongoing political change, and the extent to which the multi-stakeholder group has undertaken actions to resolve barriers encountered;
- The good faith efforts undertaken by the multi-stakeholder group to comply with the requirements;
- The reasons and justifications for not complying with the requirements; and
- Any plans agreed by the multi-stakeholder group to address the requirements in the future.

In addition to the assessment of the requirements, Validation will document:

- **Efforts to go beyond the EITI Requirements.** This will include efforts by the multi-stakeholder group to address 'encouraged' or 'recommended' aspects of the EITI Standard. It will also include efforts by the multi-stakeholder group to successfully achieve any work plan objectives that fall outside the scope of the EITI Standard, but that have been identified by the multi-stakeholder group to be necessary objectives for the EITI to address national priorities for the extractive sector. These efforts will be documented in the Validation process but will not be taken into account in assessing compliance with the EITI Standard. Where Validation concludes that the multi-stakeholder group has comprehensively implemented 'encouraged' or 'recommended' aspects of the EITI Standard, and/or work plan objectives, the EITI Board will recognise these efforts in the assessment card.
- The direction of progress towards meeting each EITI Requirement as compared to the country's previous Validation(s), indicating whether implementation is improving or deteriorating.

In accordance with the standard Terms of Reference for Validations, the results of the assessment will be documented in an assessment card and a narrative report, presenting the evidence, stakeholder views, references and conclusions.

Article 5 – Safeguards.

If a country has made inadequate progress or less on any one of the requirements relating to stakeholder engagement (Requirements 1.1, 1.2 and 1.3), the Board will suspend the country in accordance with Article 8.

If, on the first Validation, a country has made meaningful progress on Requirement 1.3 on civil society due to a deficiency related to the civil society protocol, the country will not be suspended and will be expected to demonstrate progress in addressing the corrective actions established by the Board. Failure to demonstrate progress in addressing the corrective actions in subsequent Validations will result in suspension in accordance with Article 8.

Article 6 – Outcome of Validations.

Where Validation verifies that a country has made satisfactory progress on all of the requirements, the EITI Board will designate that country as having achieved satisfactory progress overall. Implementing countries must maintain adherence to the EITI Principles and Requirements in order to retain this status. Where concerns are raised about whether implementation of the EITI has subsequently fallen below the required standard, the EITI Board reserves the right to require the country to undergo a new Validation. Stakeholders may petition the EITI Board if they consider that status should be reviewed. This request may be mediated through a stakeholder's constituency representative(s) on the EITI Board. The EITI Board will review the situation and exercise its discretion as to whether to require an earlier Validation. Subject to the findings of that assessment, the EITI Board will determine the country's status.

The consequences of not achieving satisfactory progress depend on the Board's overall assessment:

i. **No progress.** The country will be delisted.

ii. **Inadequate progress.** The country will be temporarily suspended and requested to undertake corrective actions until the second Validation. For the suspension to be lifted, the country must in its second Validation demonstrate at least meaningful progress.

    If a country achieves meaningful progress in the second Validation, the procedure in provision (iii)(2) below applies. If the country achieves inadequate progress, in the second Validation the procedure in provision (i) above applies.

iii. **Meaningful progress.** The country will be considered an EITI country and requested to undertake corrective actions until the second Validation.

    (1) If the country achieves meaningful progress overall in the second Validation, **but with no improvements on individual requirements**, the country will be temporarily suspended and requested to undertake corrective actions until the third Validation. If the country achieves meaningful progress overall in the third Validation but with no improvements on individual requirements, the country will be delisted. If the country achieves meaningful progress overall in the third Validation, but with considerable improvements across several individual requirements (i.e. several but not all requirements that were previously unmet have been met), the country will remain suspended. The Board will establish new corrective actions. Failure to meet all requirements (i.e., address all the outstanding corrective actions) in the fourth Validation will result in delisting.

    (2) If the country achieves meaningful progress overall in the second Validation, and **with considerable improvements across several individual requirements** (i.e. several but not all requirements that were previously unmet have been met), the country will be considered an EITI country whilst undertaking corrective actions. If the country achieves meaningful progress overall in the third Validation, the country will be temporarily suspended. The Board will establish new corrective actions. Failure to meet all requirements (i.e., address all the outstanding corrective actions) in the fourth Validation will result in delisting.

PH-671

ARTICLE 6. iii. CONTINUED

(3) If the country achieves inadequate progress in the second or subsequent Validations, the procedure in point (i) above applies.

Where Validation verifies that a country has not achieved compliance, the EITI Board will establish the corrective actions that the country is required to undertake and a time frame of 3-18 months for the next Validation, where progress with meeting the corrective actions will be assessed. In establishing the time frame for completing the corrective actions, the EITI Board will consider the nature of the corrective actions and local circumstances. The Board retains the right to establish shorter or longer time frames.

An implementing country may request an extension of this time frame in accordance with Article 7. A country may also request to commence Validation earlier than scheduled by the EITI Board.

An implementing country may maintain a level of overall progress that is less than satisfactory for a maximum of seven years from the date that the country was designated as an EITI country.

Article 7 – Extensions.

An implementing country may apply for an extension if it is unable to meet any of the deadlines specified above. The EITI Board will apply the following tests in assessing any extension requests:

1. The request must be made in advance of the deadline and be endorsed by the multi-stakeholder group.
2. The multi-stakeholder group must demonstrate that it has been making continuous progress towards meeting the deadline and has been delayed due to exceptional circumstances. In assessing continuous progress, the EITI Board will consider:
   i. The EITI process, in particular the functioning of the multi-stakeholder group and clear, strong commitment from government.
   ii. The status and quality of EITI reporting, including meaningful progress in meeting the requirements for timely reporting as per Requirement 4.8 and efforts to address recommendations for improving EITI reporting.
3. The exceptional circumstance(s) must be explained in the request from the multi-stakeholder group.
4. No extensions will be granted which would increase the maximum candidature period.

Article 8 – Suspension.

a) Suspension due to breaches of the EITI Principles and Requirements

Where it is manifestly clear that a significant aspect of the EITI Principles and Requirements are not adhered to by an implementing country, the EITI Board will suspend or delist that country. This includes cases where a country has not met the requirements for timely EITI reporting and/or achieving compliance with the EITI Requirements by the deadlines established by the EITI Board. Where the EITI Board is concerned that adherence to the EITI Principles and Requirements is compromised, it may task the International Secretariat with gathering information about the situation and submitting a report to the EITI Board.

Suspension of an implementing country is a temporary mechanism and is subject to the maximum candidature period. The EITI Board shall set a time limit for the implementing country to address breaches of the EITI Standard. During the period of suspension, the country will have the status "suspended". If the matter is resolved to the satisfaction of the EITI Board by the deadline, the country's status and level of progress will be reinstated. If the matter has not been resolved to the satisfaction of the EITI Board by the deadline, the EITI Board will delist the country.

b) Suspension due to political instability or conflict

The EITI Board may decide to suspend countries in cases where political instability or conflict manifestly prevents the country from adhering to a significant aspect of the EITI Principles and Requirements. Countries that are experiencing exceptional political instability or conflict may also voluntarily apply to be suspended. In this situation, the government should lodge an application for voluntary suspension with the EITI Board. The government's application should note the views of the multi-stakeholder group.

Where countries are suspended due to political instability or conflict, the period that the country is suspended will not be counted as part of the maximum candidature period. The EITI Board will monitor and review the situation on a regular basis and retains the right to extend the suspension period or delist the country.

c) Lifting the suspension

The government may apply to have the suspension lifted at any time. The application should document the steps agreed by stakeholders to restart the EITI implementation and Validation process, and the work plan to achieve compliance. If the EITI Board is satisfied that the reasons for suspension have been addressed, the suspension will be lifted. Upon lifting a suspension, the EITI Board will consider setting new reporting and Validation deadlines as appropriate. At all stages in the process, the EITI Board shall ensure its concerns and decisions are clearly communicated to the implementing country.

PH-673

Article 9 – Delisting.

Delisting, i.e. revoking a country's status as an EITI implementing country, will occur if:

(1) An implementing country has been subject to suspension and the matter has not been resolved to the satisfaction of the EITI Board by the agreed deadline.

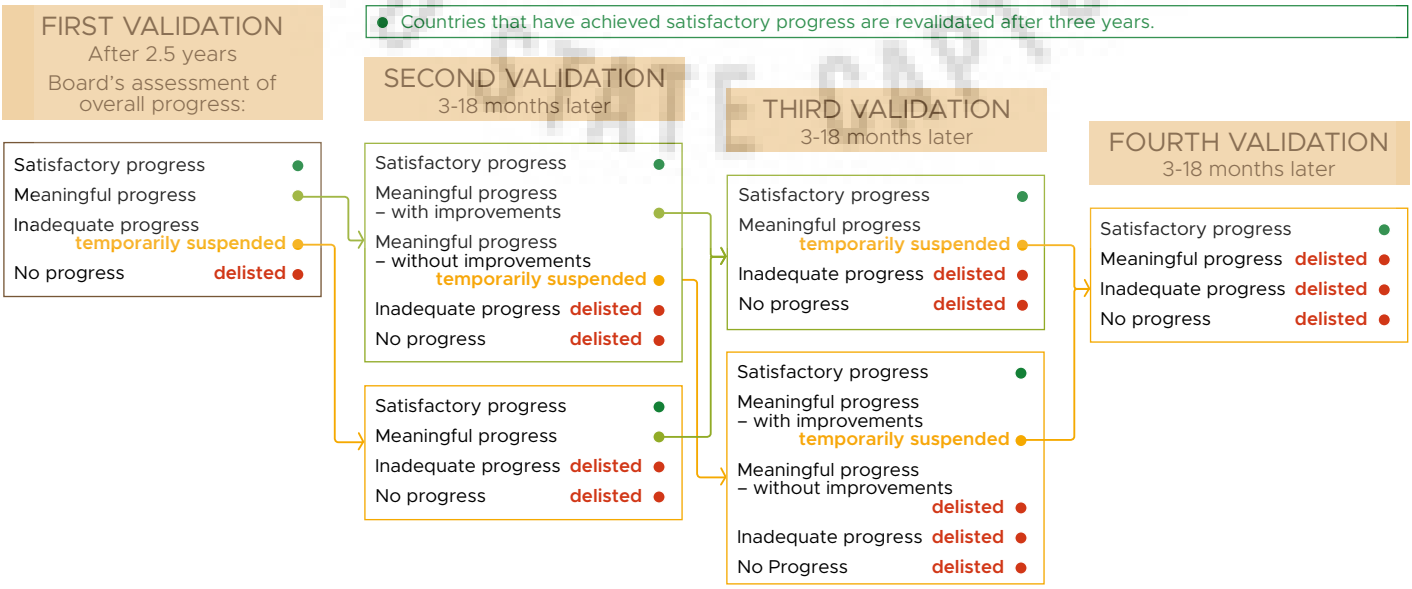
(2) The EITI Board concludes that a country has not made satisfactory progress in implementing the EITI within the established time frames.

Where it is manifestly clear that a significant aspect of the EITI Principles and Requirements are not adhered to by an implementing country, the EITI Board reserves the right to delist the country. A delisted country may reapply for admission as an EITI country at any time. The EITI Board will apply the agreed procedures with respect to assessing EITI country applications. It will also assess previous experience in EITI implementation, including previous barriers to effective implementation, and the implementation of corrective measures.

Article 10 – Appeals.

The implementing country concerned may petition the EITI Board to review its decision regarding suspension, delisting or the country designation as having made meaningful or satisfactory progress following Validation. In responding to such petitions, the EITI Board will consider the facts of the case, the need to preserve the integrity of the EITI, and the principle of consistent treatment between countries. The EITI Board's decision is final. The country concerned may, prior to the notice periods under Article 7 of the Articles of Association, appeal a decision of the EITI Board to the next ordinary Members' Meeting.

Outcomes and consequences of Validation



PH-674

5. Overview of Validation

This section is concerned with EITI Validation. The purpose of Validation is to assess compliance with the EITI Requirements set out in section 3.

Validation objectives

Validation is an essential feature of the EITI process. It serves to assess performance and promote dialogue and learning at the country level. It also safeguards the integrity of the EITI by holding implementing countries to the same global standard. It is intended to provide all stakeholders with an impartial assessment of whether EITI implementation in a country is in line with the provisions of the EITI Standard. The Validation report, in addition, seeks to identify the impact of the EITI in the country being validated, the implementation of activities encouraged by the EITI Standard, lessons learnt in EITI implementation, as well as any concerns stakeholders have expressed and recommendations for future implementation of the EITI.

Validation methodology

Validation assesses progress towards the EITI Requirements set out in section 3. The methodology is set out in the Validation Guide, with guidance on assessing each provision of the EITI Standard. In some cases, the Validation Guide specifies the evidence that the validator must use to ensure that a provision has been satisfied. In other cases, there are different approaches that a country might take to address an EITI provision, and the Validation Guide provides examples of the types of evidence that the validator might consider.

Validation procedure

Given the multi-stakeholder nature of the EITI and the importance of dialogue, the Validation procedure emphasises stakeholder consultation. Validation is carried out in four stages.

1. **Preparation for Validation.** Prior to the commencement of Validation, the multi-stakeholder group is encouraged to undertake a self-assessment of adherence to the EITI Standard. The Validation Guide includes a provision that: "where the multi-stakeholder group wishes that Validation pays particular attention to assessing certain objectives or activities in accordance with the multi-stakeholder group work plan, these should be outlined upon the request of the multi-stakeholder group ". The national secretariat is requested to collate the documentation and other sources that demonstrate compliance, including multi-stakeholder group minutes. Stakeholders are also invited to prepare any other documentation they consider relevant. A guidance note on preparing for Validation is available[5].

5 Available from the International Secretariat and on eiti.org/guide, guidance note 23.

PH-675

VALIDATION PROCEDURE CONTINUED

2. **Initial data collection and stakeholder consultation undertaken by the EITI International Secretariat.** The International Secretariat reviews the relevant documentation, visits the country and consults stakeholders. This includes meetings with the multi-stakeholder group, the Independent Administrator and other key stakeholders, including stakeholders that are represented on, but not directly participating in, the multi-stakeholder group. The Board maintains a standardised procedure for data collection, addressing stakeholder consultation and deadlines for the completion of the initial assessment.

   Based on these consultations, the International Secretariat will prepare a report making an initial evaluation of progress towards requirements in accordance with the Validation Guide. The initial assessment will not include an overall assessment of compliance.

   The report is submitted to the Validator. The National Coordinator receives a copy. Comments on the facts are welcome but National Coordinators and the multi-stakeholder group are encouraged to defer any major commentary until they receive the Validator's draft report.

3. **Independent Validation.** The Board will appoint an Independent Validator through an open, competitive tendering process. The Validator will report to the Board via the Validation Committee.

   The Validator assesses whether the Secretariat's initial assessment has been carried out in accordance with the Validation Guide. This will include: a detailed desk review of the relevant documentation for each requirement and the Secretariat's initial evaluation for each requirement, and a risk-based approach for spot checks, and further consultations with stakeholders. The Board may request that the Validator undertake spot checks on specific requirements.

   The Validator comments on the Secretariat's initial assessment and prepares a Draft Validation Report. The multi-stakeholder group is invited to comment on the Draft Validation Report. Having considered the multi-stakeholder group's comments, the Validator compiles a Final Validation Report. The Validator writes to the multi-stakeholder group to explain how it has considered their comments. The multi-stakeholder group receives a copy of the Final Validation Report.

   The Final Validation Report will include the Validator's assessment of compliance with each provision, but not all overall assessment of compliance. The Validator will be invited to present their findings to the Validation Committee.

4. **Board Review.** The Validation Committee will review the Final Validation Report and the supporting documentation (including the multi-stakeholder group's comments). The Validation Committee will then make a recommendation to the EITI Board on the country's compliance with the EITI Requirements and, where applicable, any corrective actions required.

VALIDATION PROCEDURE CONTINUED

The EITI Board will make the final determination of whether the requirements are met or unmet, and on the country's overall compliance in accordance with Article 6 of the EITI Board's procedures for oversight of EITI implementation.

The initial assessment, Validation Report and associated multi-stakeholder group comments are considered confidential until the Board has reached a decision.

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-677

6. Protocol: Participation of civil society

1. Introduction

The participation of civil society is fundamental to achieving the objectives of EITI, including Principle 4 which states that "public understanding of government revenues and expenditure over time could help public debate and inform choice of appropriate and realistic options for sustainable development". The active participation of civil society in the EITI process is key to ensure that the transparency created by the EITI leads to greater accountability. A primary motivation for the adoption of the EITI Standard was the desire to produce more relevant, more reliable and more usable information, and better link this information to wider reforms in the governance of the extractive sector or of the management of public accounting and revenue management. Citizens' ability to work actively to make use of the information generated by the EITI is therefore a critical component of EITI implementation and civil society participation in the EITI.

The participation of civil society in the EITI process is formally assessed at two stages of EITI implementation – during the candidature assessment and during the Validation process. An assessment of civil society participation may also take place on an ad hoc basis in response to specific concerns raised with the Board about the situation in specific implementing countries. This protocol sets out the questions the EITI Board (including Committees) and validators should consider in assessing whether the provisions pertaining to civil society participation (Requirement 1.3) have been met, as well as the types of evidence to be used in answering those questions. While the provisions relating to civil society participation in the EITI process remain consistent at every stage of EITI implementation, the evidence the EITI Board uses to evaluate the provisions will of necessity vary depending on the circumstances of the country, stage of implementation, and availability of information. It should be noted that the questions posed and the suggested types of evidence set out in 2.1-2.5 below do not constitute provisions, nor is the list exhaustive. However, it provides an assessment framework for the provisions related to civil society.

2. The EITI's interpretation of the provisions on civil society

For purposes of this protocol, references to 'civil society representatives' will include civil society representatives who are substantively involved in the EITI process, including but not limited to members of the multi-stakeholder group. References to the 'EITI process' will include activities related to preparing for EITI sign-up; multi-stakeholder group (MSG) meetings; CSO constituency side-meetings on EITI, including interactions with MSG representatives; producing EITI Reports; producing materials or conducting analysis on EITI Reports; expressing views related to EITI activities; and expressing views related to natural resource governance.

In assessing the civil society provisions, the Board and validators will apply the following tests:

2.1 Expression: Civil society representatives are able to engage in public debate related to the EITI process and express opinions about the EITI process without restraint, coercion or reprisal.

The EITI Board and validators will consider the extent to which:

- Civil society representatives are able to speak freely in public about the EITI process including for example during MSG meetings, EITI events including for the promulgation of EITI Reports, public events, in the media etc.
- Actual practice, including diverse stakeholder views or substantive evidence provided by independent third parties, indicates that self-censorship or self-imposed restriction by civil society representatives has taken place related to the EITI process due to fear of reprisal and whether such barriers have impacted civil society representatives' dissemination of information and public comment on the EITI process.

2.2 Operation: Civil society representatives are able to operate freely in relation to the EITI process.

The EITI Board and validators will consider the extent to which the legal, regulatory, administrative and actual environment has affected civil society representative's ability to participate in the EITI process. This could for example include:

- The extent to which legal, regulatory or administrative obstacles affecting the ability of civil society representatives to participate in the EITI process. This could include legal or administrative procedures related to the registration of CSOs that have adversely affected their ability to participate in the EITI process; legal or administrative restrictions on access to funding that have prevented CSOs from undertaking work related to the EITI process; legal or administrative issues preventing CSOs from holding meetings related to the EITI process, legal or administrative barriers to the dissemination of information and public comment on the EITI process etc.
- Any evidence suggesting that the fundamental rights of civil society representatives have been restricted in relation to the implementation of the EITI process, such as restrictions on freedom of expression or freedom of movement.

2.3 Association: Civil society representatives are able to communicate and cooperate with each other regarding the EITI process.

The EITI Board and validators will consider the extent to which:

- Civil society MSG representatives may seek and are not restricted from engaging other CSOs that are not part of the MSG, including capturing their input for MSG discussions and communicating outcomes of MSG deliberations.

PH-679

- Formal or informal communication channels between civil society MSG members and the wider civil society constituency have not been restricted.
- Civil society MSG representatives have not been restricted from engaging in outreach to broader civil society, including related to discussions about MSG representation and the EITI process.

2.4 Engagement: Civil society representatives are able to be fully, actively and effectively engaged in the design, implementation, monitoring and evaluation of the EITI process.

The EITI Board and validators will consider the extent to which:

- Civil society representatives are able to fully contribute and provide input to the EITI process. This could for example include evidence of input and advocacy related to key MSG deliberations on issues such as work plan objectives and activities, the scope of the EITI reporting process, approval of EITI Reports, annual self-assessment of the EITI process through the annual activity reports, Validation etc. It could also include evidence that civil society is regularly participating in MSG meetings, MSG working groups and other EITI events, and that the views of CSOs are taken into account and documented in MSG meeting minutes.
- Civil society representatives consider that they have adequate capacity to participate in the EITI. This should include evidence that technical, financial or other capacity constraints affecting civil society have been considered and that plans for addressing such constraints have been agreed upon and/or effectuated including by providing access to capacity building or resources.

2.5 Access to public decision-making: Civil society representatives are able to speak freely on transparency and natural resource governance issues, and ensure that the EITI contributes to public debate.

The EITI Board and validators will consider the extent to which:

- Civil society representatives are able to use the EITI process to promote public debate for example through public events, workshops and conferences organised by or with participation of civil society to inform the public about the EITI process and outcomes.
- Civil society representatives are able to engage in activities and debates about natural resource governance, including for example conducting analysis and advocacy on natural resource issues, use of EITI data, engagement with media outlets, development of tools to communicate the findings of the EITI Reports, etc.

2.6 Available documentation from the MSG and CSOs engaged in the EITI process as well as outcomes from direct consultation with relevant stakeholders, including but not limited to members of the MSG, should be taken into account when gathering the above evidence. For contextual purposes, the EITI Board will review the broader environment in which the EITI operates for example by reference to indicators or other types of assessments relevant to the issues addressed in 2.1-2.5 above.

3. Ad-hoc restrictions on civil society representatives

3.1 Ad hoc allegations or reports of potential or actual restrictions on civil society representatives in EITI implementing countries should in the first instance be discussed and addressed by the multi-stakeholder group, subject to any safety concerns that an impacted party may have regarding directly raising such issues domestically.

3.2 The EITI Board through its Rapid Response Committee may be called to investigate particular cases and address alleged breaches of the EITI Principles and Provisions as appropriate. The EITI Board will consider such requests with regard to the facts of the case, the need to uphold the Principles of the EITI as well as the principle of consistent treatment between countries. In accordance with section 4, Article 8.a), "where the EITI Board is concerned that adherence to the EITI Principles and Provisions is compromised, it may task the International Secretariat with gathering information about the situation and submitting a report to the EITI Board". Where concerns related to the participation of civil society are raised, the EITI Board will as appropriate strive to establish whether there is a direct link to the EITI process, including by (i) documenting the facts of the case; (ii) gathering stakeholders' views; and (iii) applying the test set out in section 2 above.

3.3 Depending on the circumstances of the case including the extent to which it can be established that there is a direct link between the concerns raised and the EITI process, the Board will consider an appropriate response. This could for example include a letter from the Chair or the EITI Board to the government concerned, EITI Board or International Secretariat missions to the country, commissioning independent assessments, issuing Board declarations, agreeing to remedial actions including monitoring of implementation, or calling for a validation of a country's adherence to the provisions concerned. In accordance with section 4, Article 8.a), "where it is manifestly clear that a significant aspect of the EITI Principles and Provisions are not adhered to by an implementing country, the EITI Board will suspend or delist that country. In cases where the Board concludes that the concerns observed do not breach a provision or are not sufficiently linked to the EITI process, it will exercise its discretion as to whether to take any action, placing priority on the need to uphold the Principles of the EITI and to ensure consistent treatment between countries.

PH-681

7. Expectations for EITI supporting companies

All EITI supporting companies are expected to:

- Publicly declare support for the EITI Principles and, by promoting transparency throughout the extractive industries, help public debate and provide opportunities for sustainable development.
- As a guiding principle, supporting companies are expected to publicly disclose taxes and payments. Where companies choose not to, they should state why.
- Ensure comprehensive disclosure of taxes and payments made to all EITI implementing countries.
- In accordance with EITI beneficial ownership requirements, publicly disclose beneficial owners and take steps to identify the beneficial owners of direct business partners, including Joint Ventures and contractors. Listed companies will do what is required by applicable regulations and listing requirements.
- Engage in rigorous procurement processes, including due diligence in respect to partners and vendors.
- Support the operationalisation of countries' decisions to disclose future licenses and contracts entered into that govern the exploration and exploitation of oil, gas and minerals in accordance with the recommendations in the EITI Standard. Companies recognise that achievement of greater transparency must be set in the context of respect for contracts and laws in accordance with the EITI Principles.
- Companies, working together with governments, to deliver natural resources in a manner that benefits societies and communities.
- Ensure that company processes are appropriate to deliver the data required for high standards of accountability.

PH-682

8. Open data policy

Preamble

1. This policy contains recommendations on open data in implementation of the EITI within the agreed scope of EITI implementation at the national level. It complements the requirements regarding open data as per Requirement 7. It builds on lessons emerging from national level implementation and emerging international best practice[6] and encourages systematic disclosure[7].
2. The EITI Principles declare that "a public understanding of government revenues and expenditure over time [can] help public debate and inform choice of appropriate and realistic options for sustainable development" (EITI Principle 4). The EITI Standard therefore requires EITI disclosures to be "comprehensible, actively promoted, publicly accessible, and contribute to public debate" (EITI Requirement 7.1). Improving the accessibility, reliability, relevance, timeliness and comparability of EITI data is essential to realise these objectives.
3. To help realise the EITI Principles, the EITI Board has agreed that systematic disclosure of EITI data through government and company systems is now the default expectation[8]. The EITI encourages routine disclosure from the reporting entities in open formats at the national level within the agreed scope of EITI implementation[9].
4. The EITI acknowledges that the circumstances differ in each implementing country, that not all countries will be able to transition to open data at the same speed, and that the financial implications need to be considered, both in the near and long term. The demand from the public and the use of the data to address public policy issues should be considered[10]. Access challenges and information needs of different genders and subgroups of citizens should also be taken into account.

Open data objectives

5. Open data from EITI implementation can improve transparency about government and business activities and increase awareness about how countries' natural resources are governed. It can shed light on who owns extractives companies, who holds licenses and permits, what the relevant fiscal terms are and what extractives revenues are levied and spent. Such disclosures provide strong incentives for that money to be used most effectively.

---

6 Including the Open Government Partnership, the G8 Open Data Charter and Technical Annex, the Open Data Charter (http://opendatacharter.net/), the open definition (http://opendefinition.org/) and the World Wide Web Consortium (W3C) for developing data standards (https://www.w3.org/Consortium)

7 See https://eiti.org/BD/2018-8

8 Ibid.

9 See Requirement 4

10 The key is to "publish with purpose", meaning that data publication should be embedded to solving specific policy problems.

PH-683

6. Open data is effective and useful when it is timely, of good quality, addressing stakeholder needs and expectations. EITI implementation should promote accountability and good governance, enhance public debate and citizen engagement, help combat corruption through enhanced government accountability and improve the delivery of government services. Providing access to comprehensive data can empower individuals, the media, civil society, and business to make better informed choices about the services they receive and the standards they should expect. Open data can also be a valuable tool for government in improving policy making and sector management.
7. Free access to, and subsequent re-use of, open data are of significant value to society and the economy. It can be a valuable source of information to multi-stakeholder groups in EITI implementing countries.
8. Emerging data standards can contribute to making data interoperable. Adopting data standards[11] also contributes to the sustainability of data publishing, supports the capacity of governments, industry and civil society to prepare and publish data through accessing existing tools and resources, and can support data use and analysis where standards are thoughtfully designed, and communities of users form around them.

Open data in EITI Implementation

9. EITI Implementing countries are encouraged to:
   a) systematically publish open data by embedding open data policies and strategies in reporting entities involved in EITI reporting to ensure timely and quality data, accessibility and cost effectiveness of data delivery;
   b) working with users[12] to identify priority data sets and the form that the data delivery should take;
   c) consider different user needs and access challenges based on gender, ethnic and geographic representation;
   d) ensure that data are provided in granular, machine-readable formats and fully described, so that users have sufficient information to understand their strengths, weaknesses, analytical limitations and security requirements, as well as how to process the data;
   e) release data as early as possible, allow users to provide feedback, and then continue to make revisions to ensure the highest standards of open data quality.

11 Examples include: for beneficial ownership, the beneficial ownership data standard is emerging as an open data standard (http://standard.openownership.org); for contracts the Open Contracting Data Standard is being adopted (http://standard.open-contracting.org/).

12 Users can refer to citizens, the media, academia and of course other government agencies who use data from other agencies for their own service delivery.

f) release data under an open license, preferably CC 4.0[13], that allows users to freely obtain and easily re-use it[14];

g) share technical expertise and experience with other countries to maximise the potential of open data in a socially inclusive manner;

h) work to increase open data literacy and encourage people, such as developers of applications and civil society organisations that work in the field of open data promotion, to unlock the value of open data;

i) ensure that data is interoperable with national and international standards[15], including adopting data standards approved by the EITI Board and additional guidance provided by the EITI International Secretariat;

j) where possible support the cross-referencing of data with other datasets by using unique, persistent and public identifiers for commercial and government entities;

k) consider the technical infrastructure to deliver and use the open data[16];

l) consider the governance and sustainability of open data policies as to ensure that reporting entities have a data steward, data is retained, and security standards are in place.

Engagement with the open data community

10. To learn from and shape best practices of government open data, EITI countries are encouraged to endorse the Open Data Charter[17] and other relevant initiatives[18];

11. To transfer lessons learned from EITI countries and draw from international experience the EITI International Secretariat should engage in working groups focussing on open data, where considered complementary[19].

13 See https://creativecommons.org/licenses/by/4.0/ and https://creativecommons.org/licenses/by/4.0/legalcode

14 See 'Recommendations for licensing' suggested by Open Knowledge International https://research.okfn.org/avoiding-data-use-silos/#the-licensing-process

15 See, for example, the open data standards directory http://datastandards.directory/

16 Technical infrastructure relates to the information technology and skills needed to enable data to be collected, cleaned, connected to other datasets and published. Mapping data ecosystems can be a way to chart out the technical infrastructure and actors related to the collection, curation and publication of data. See for example Open Data Institute's guide https://theodi.org/project/mapping-data-ecosystems/ and the DFID principles for digital development: https://digitalprinciples.org/principle/understand-the-existing-ecosystem/

17 See open data charter: https://opendatacharter.net/endorse-the-charter/

18 Such as the guidelines "Principles for Digital Development": https://digitalprinciples.org/

19 For example, Open Data Charter's implementation working group, which develops tools and resources to support governments in the implementation of open data and promotes and facilitates peer learning across countries and organisations. See https://opendatacharter.net/who-we-are/ for more background.

PH-685

CHAPTER II
Governance and management

The EITI has evolved into a global standard which provides a platform for wider debate and reform. The governance and management of the EITI itself has also evolved. The EITI is governed by a not-for-profit members association under Norwegian law. It is the EITI Association's articles that provide the governing framework for the EITI.

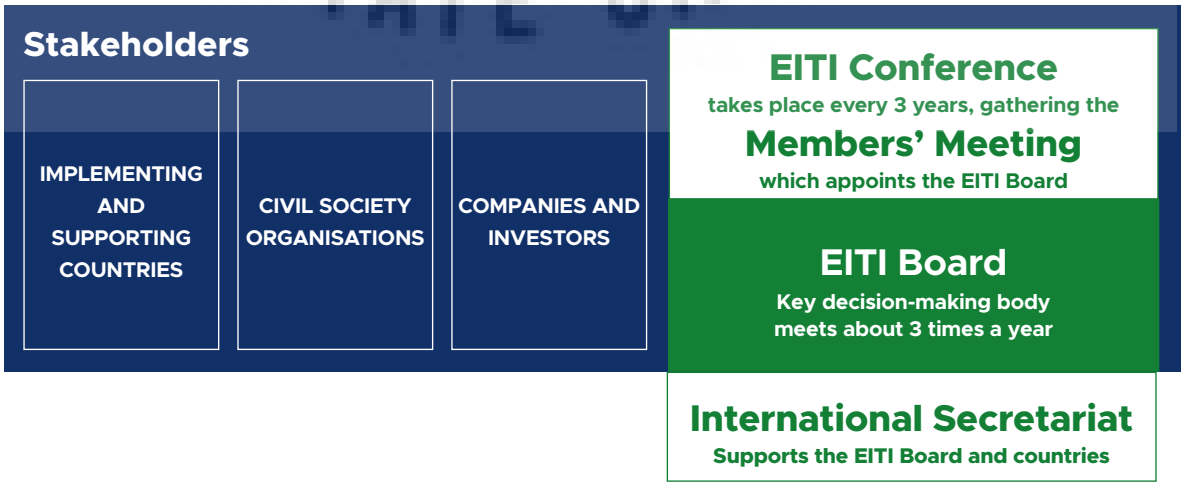
The EITI arranges a Global Conference at least every three years, in order to provide an international forum for EITI stakeholders to further the objectives of the EITI. Alongside these Conferences, a smaller Members' Meeting with the three constituency groups – countries (implementing and supporting), companies (including financial institutions) and civil society organisations – takes place. The votes of the three constituencies are equally balanced. A main task of the Members' Meeting is to appoint the EITI Board. Constituencies agree among themselves their membership of the Association and who they wish to nominate to the EITI Board.

Between these Conferences and the Members' Meetings, the EITI Board oversees the activities of the EITI through regular Board meetings, committee meetings and frequent Board circulars. The EITI Board has 21 members, with the different constituencies being entitled to representation.

The EITI International Secretariat is responsible for the day-to-day running of the EITI Association. A considerable amount of technical assistance is provided to countries implementing the EITI both by the EITI International Secretariat and other multilateral, bilateral and non-governmental organisations.

This section contains the main documents concerning the governance of the EITI at the international level:

- Articles of Association, to be approved at the Members' Meeting on 17 June 2019
- Openness Policy which sets out how the EITI itself should be transparent
- EITI Constituency guidelines available at eiti.org/governance
- EITI Association code of conduct



PH-686

9. Articles of Association

Subject to agreement by the EITI Members meeting on 17 June 2019. If these are not approved, the 2016 Articles remain in place.

ARTICLE 1 NAME

1. The name of the association shall be "The Association for the Extractive Industries Transparency Initiative (EITI)" (hereinafter referred to as "the EITI Association").

ARTICLE 2 BACKGROUND AND OBJECTIVE

1. The EITI Association is an international multi-stakeholder initiative with participation of representatives from governments and their agencies; oil, gas and mining companies; asset management companies and pension funds (hereinafter referred to as "Institutional Investors") and local civil society groups and international non-governmental organisations.
2. The objective of the EITI Association is to make the EITI Principles and the EITI Requirements the internationally accepted standard for transparency in the oil, gas and mining sectors, recognising that strengthened transparency of natural resource revenues can reduce corruption, and the revenue from extractive industries can transform economies, reduce poverty, and raise the living standards of entire populations in resource-rich countries.

ARTICLE 3 LEGAL PERSON, LIMITED LIABILITY

1. The EITI Association is a non-profit association organised under Norwegian law ("forening").
2. The Members of the EITI Association shall not be responsible, individually or collectively, for any of the EITI Association's debts, liabilities or obligations.

ARTICLE 4 ORGANISATION

1. The permanent institutional bodies of the EITI Association are:
   i. The EITI Members' Meeting, which is held in connection with the EITI Conference;
   ii. The EITI Board led by the EITI Chair;
   iii. The EITI Secretariat led by the Executive Director;
2. The EITI Board may establish committees in accordance with Article 14;
3. The EITI Association's organisation operates transparently and encourages diversity in terms of gender, nationalities and culture.

PH-687

ARTICLE 5 MEMBERSHIP AND CONSTITUENCIES

1. A Member of the EITI Association is a personal representative of a country (meaning state), company, organisation or legal entity that is appointed by a Constituency as set out in Articles 5 (2) and (3).

2. The Members are organised in three Constituencies which are:
   i. The Constituency of Countries, which comprise:
      a) Implementing Countries, meaning states, that have been classified by the EITI Board as such; and
      b) Supporting Countries, meaning states or union of states, that support the objective of the EITI Association as defined by the EITI Board.
   ii. The Constituency of Companies, which comprise:
      a) Companies in the extractive sector that have committed to support the objective of the EITI Association as defined by the EITI Board and associations representing these companies;
      b) Institutional Investors that have committed to support the objective of the EITI Association as defined by the EITI Board; and
      c) Commodity traders that have committed to support the objective of the EITI Association as defined by the EITI Board.
   iii. The Constituency of Civil Society Organisations, which comprise non-governmental organisations, global action networks or coalitions that support the objective of the EITI Association as defined by the EITI Board.

3. Each Constituency decides on its rules governing appointments of Members of the EITI Association. The Membership shall be limited to the following:
   i. From the Constituency of Countries, up to one representative from each Implementing Country and each Supporting Country (or their unions);
   ii. From the Constituency of Companies, up to one representative from each company and associations representing them, and a maximum of five representatives from Institutional Investors;
   iii. From the Constituency of Civil Society Organisations, up to one representative from each Civil Society Organisations.

4. A Constituency may replace any of its own appointed Members at any time. The Constituency shall inform the EITI Secretariat of its Members at any time.

5. The EITI Board may terminate any Member's Membership of the EITI Association if:
   i. The Member, or the country or other entity the Member represents, does not comply with these Articles of Association; or
   ii. The Member, or the country or other entity the Member represents, has conducted his/her/its affairs in a way considered prejudicial or contrary to the EITI Principles.

6. A resolution by the EITI Board in accordance with Article 5 (5) may be appealed by any Member to the Members' Meeting for final decision.

ARTICLE 6 THE EITI CONFERENCE

1. An EITI Conference shall be held at least every three years in order to provide a forum for EITI stakeholders, being all with an interest in the EITI Association, to further the objective of the EITI Association and to express their views on the policies and strategies of the EITI Association. The EITI Chair shall act as chairman for the Conference. The EITI Conference is a non-governing body of the EITI Association.

2. The EITI Members, the EITI Board and the EITI Secretariat have the right to attend or be represented at the EITI Conference. Other EITI stakeholders should also be invited, in each case, to the extent that it is reasonably practical to make arrangements in order to do so as decided by the EITI Board.

3. The EITI Conference shall be summoned by the EITI Board on the EITI website and by written notice to the Members and Constituencies with at least four weeks' notice. The written notice shall include the agenda of the EITI Conference.

4. The EITI Conference shall:
   i. Provide an important and visible platform for debate, advocacy, continued fund raising, and inclusion of new EITI stakeholders;
   ii. Review progress based on the activity report for the period since the preceding ordinary Members' Meeting;
   iii. Provide suggestions to the EITI Board as to the activities of the EITI Association until the next ordinary Members' Meeting;
   iv. Mobilise and sustain high level coordination, political commitment and momentum to achieve the objective of the EITI Association; and
   v. Provide an informal communication channel for those EITI stakeholders who are not formally represented elsewhere in the governance structure of the EITI Association.

5. Views on the issues set out in Article 7 (4) above may be expressed in a non-binding Statement of Outcomes which shall be agreed upon by the EITI Conference and communicated to the EITI Members' Meeting and the EITI Board. The EITI Conference shall make every effort to adopt resolutions by consensus. Taking account of the view of the EITI stakeholders, the EITI Chair may decide that a vote is required. Every EITI stakeholder, except the Members of the EITI Board in this capacity and the Secretariat, has one vote. Resolutions of the EITI Conference are adopted by simple majority of those present and voting.

PH-689

ARTICLE 7 THE EITI MEMBERS' MEETING

1. The governing body of the EITI Association is the EITI Members' Meeting.
2. The EITI Members' Meeting is comprised of the Members of the EITI Association.
3. The ordinary EITI Members' Meeting shall be held at least every three years in connection with the EITI Conference. The ordinary EITI Members' Meeting shall be summoned by the EITI Board to the Members with at least four weeks written notice.
4. An Extraordinary Members' Meeting may be summoned by the EITI Board to the Members with at least three weeks written notice. The EITI Board shall ensure that an Extraordinary Members' Meeting shall be held within four weeks of the receipt by the EITI Chair of a request to hold an Extraordinary Members' Meeting.
5. Members who wish to take part in an EITI Members' Meeting, must give notice to the EITI Secretariat by the date stated in the summons. A Member may be represented in the EITI Members' Meeting by written proxy. The proxy may also include specific voting instructions.

   A duly signed proxy must be received by the EITI Secretariat by the date stated in the summons.
6. The EITI Chair shall act as chairman for the EITI Members' Meeting.
7. The quorum of a Members' Meeting shall be a minimum of one third of the Members, and must include at least one third of the Members from each Constituency.
8. The Members' Meeting shall make every effort to adopt resolutions by consensus. If a vote is required, resolutions are adopted by qualified majority requiring the support of at least two thirds of the total votes cast and must include the support of at least one third of the votes cast by the Members representing each Constituency. The total number of votes for the Members of each Constituency shall be equal and be determined as follows:
   i. Members from the Constituency of Countries shall have one vote each; and
   ii. The votes for Members from the Constituency of Companies and the Constituency of Civil Society Organisations shall be determined by dividing the total of Country votes by the number of Members of the Company and Civil Society Constituencies respectively.
   iii. The EITI Chair shall announce the number of votes for each Member from the different Constituencies prior to voting.

ARTICLE 8 THE FUNCTIONS OF THE EITI MEMBERS' MEETING

1. The EITI Members' Meeting shall:
   i. Approve the activities report, the accounts and the activity plan of the EITI Board;
   ii. Elect the Members, and Alternates for each Member, of the EITI Board, on nomination from the Constituencies;
   iii. Elect the EITI Chair, on proposal of the EITI Board; and

iv. Consider any other matters pursuant to requests from a Member. Such requests shall be submitted in writing to the EITI Chair in time for any such matters to be included in the agenda for the EITI Members' Meeting stated in the summons.

ARTICLE 9 THE EITI BOARD

1. The executive body of the EITI Association is the EITI Board, elected by the EITI Members' Meeting and operating under the guidance from the EITI Members' Meeting.

2. In order to reflect the multi-stakeholder nature of the EITI Association, the EITI Board shall consist of 20 EITI Board Members ("Board Members") and shall be made up as follows:
   i. A Chair;
   ii. Nine Board Members being Members of the EITI Association from the Constituency of Countries, of which a maximum of three Board Members should represent Supporting Countries and the remainder should represent Implementing Countries;
   iii. Six Board Members being Members of the EITI Association from the Constituency of Companies, of which a maximum of one should represent Institutional Investors;
   iv. Five Board Members being Members of the EITI Association from the Constituency of Civil Society Organisations.

3. All Board Members retire with effect from the conclusion of the ordinary EITI Members' Meeting held subsequent to their nomination, but shall be eligible for re-nomination at that EITI Members' Meeting.

4. The Constituencies may nominate, and the EITI Members' Meeting may elect, one alternate Board Member (an "Alternate") for each Board Member that the Constituency has nominated. An Alternate may deputise for the Board Member. If there is no Alternate, the relevant Constituency shall nominate a new Board Member and Alternate.

5. If a Board Member is absent from a Board Meeting, that Board Member's Alternate may attend, participate in discussions, vote and generally perform all the functions of that Board Member in the Board Meeting.

6. In the case of a vacancy on the EITI Board between two EITI Members' Meetings, this vacancy shall be filled by the resigning Board Member's Alternate, with the concerned Constituency nominating a new Alternate to be elected by the Board. Alternatively, the concerned Constituency may nominate a new Board Member to be elected by the Board.

7. The EITI Association shall obtain liability insurance for Board Members. The terms and conditions should be approved by the EITI Board.

8. The EITI Board may decide that a Board Member representing an implementing country that is suspended during the tenure may keep the status as a Board Member, but refrain from engaging in Board activities during the period of suspension. Should the suspension be in force for more than a year, the EITI Board may decide that the Board membership should be terminated.

PH-691

ARTICLE 10 EITI OBSERVERS

1. Representatives from relevant international organisations, such as the World Bank, the International Monetary Fund and other relevant stakeholders, should be invited by the EITI Board to attend EITI Board Meetings and Members' Meetings as observers, when this can be practically accommodated. They have no voting rights, but may be invited to express their views on specific matters. The EITI Board may decide that certain items should be discussed without observers present.

ARTICLE 11 THE EITI CHAIR

1. The EITI Chair shall be elected at the ordinary EITI Members' Meeting. The EITI Board shall, prior to each ordinary EITI Members' Meeting, recommend a candidate for the EITI Chair for the period following that EITI Members' Meeting. The term of an EITI Chair's may be renewed once.
2. The EITI Chair shall:
   i. Act as chairman of the EITI Members' Meeting;
   ii. Act as chairman of the EITI Board Meeting;
   iii. Present the EITI Board report to the EITI Conference and the EITI Members' Meeting;
   iv. Represent the EITI Board in external matters;
   v. Follow-up with the EITI Secretariat regarding the implementation of the resolutions of the EITI Board; and
   vi. Seek to foster collaborative relationships between EITI stakeholders.
3. If the EITI Chair is unable to preside over a Board Meeting, the Board Members present may appoint another Board Member to chair that Meeting.

ARTICLE 12 FUNCTIONS OF THE EITI BOARD

1. The EITI Board shall act in the best interests of the EITI Association at all times. The EITI Board shall exercise the executive powers of the EITI Association subject to the resolutions of the EITI Members' Meeting, including the following key functions:
   i. Consider general and specific policy issues affecting the EITI Association;
   ii. Agree on the work plans and budget of the EITI Association;
   iii. Agree on the arrangements for the EITI Conferences and the EITI Members' Meetings;
   iv. Present (through the EITI Chair) the activity report and the activity plan to the EITI Conference and obtain approval of the same from the EITI Members' Meeting;
   v. Present (through the EITI Chair) the annual accounts and the audit reports for the accounting periods since the last ordinary EITI Members' Meeting;
   vi. Engage the Executive Director;
   vii. Oversee and direct (through the EITI Chair) the work of the EITI Secretariat;

viii. Ensure that the multi-stakeholder nature of the EITI Association is maintained and fully reflected in the EITI Association at all levels, including in its Committees;

ix. Monitor and support implementation of the EITI in implementing countries and establish its procedures regarding the validation process, including complaints, resolving disagreements, the question of de-listing a country and appeal procedures;

x. Adopt more detailed procedures and rules for the management and operation of the EITI Association including the contents of country work plans and company work plans, the validation process, the management of funds, payments for projects, goods and services, auditing and reporting and the approval of projects;

xi. Recommend a candidate for the EITI Chair prior to each ordinary EITI Members' Meeting; and

xii. Adopt a code of conduct.

ARTICLE 13 COMMITTEES OF THE EITI BOARD

1. The EITI Board may create committees to further specific issues. Any such committee should include two or more Board Members or their Alternates, and its composition should, as far as is reasonable, reflect the multi-stakeholder nature of the EITI Association. The terms on which any such committee shall operate should be recorded in the Minute Book.

ARTICLE 14 EITI BOARD OPERATIONS AND PROCEEDINGS

1. The EITI Board should meet at least twice a year. If the circumstances so necessitate, EITI Board Meetings can be held by telephone conference. At least one EITI Board Meeting per year shall be in person.

2. A Board Meeting shall be convened by written notification from the EITI Chair with at least 14 days notice. Any shorter period of notice requires the written consent of all Board Members.

3. Board Members shall make every effort to adopt resolutions by consensus. Taking account of the view of the Board Members, the EITI Chair may decide that a vote is required. Every Member of the EITI Board has one vote. Voting can be done by written proxy.

4. No resolution may be made by a Board Meeting unless a quorum is present at the time of passing the resolution. At least two-thirds of the Board Members, with at least two Board Members from the Constituency of Countries (one Implementing Country and one Supporting Country), one Board Member from the Constituency of Civil Society Organisations and one Board Member from the Constituency of Companies, establish a quorum.

5. If a vote is required, resolutions are adopted by a qualified majority requiring 13 votes to be cast in favour of the resolution, and must include the support of at least one third of the votes of the Board Members from each Constituency.

6. A Board Member shall not vote in respect of any matter or arrangement in which he or she is directly interested, or if there are any other special

PH-693

circumstances which are apt to impair confidence in his or her impartiality. A Board Member shall declare such interests in writing to the EITI Board as soon as possible after he or she becomes aware of the same. A Board Member shall not be counted in the quorum present when any resolution is made about a matter which that Board Member is not entitled to vote upon.

7. The EITI Board may establish procedures regarding decision-making processes outside Board Meetings. Any decisions taken outside Board Meetings in accordance with such procedures should be recorded in the Minutes of the Board Meeting following when the decision was taken.

8. The EITI Association can be committed externally by the joint signature of all Board Members. The EITI Board may elect the Chair alone, or two or several Board Members to carry the right of signature, of which any two can sign jointly.

ARTICLE 15 THE EITI SECRETARIAT

1. The EITI Secretariat ("the Secretariat") shall consist of the Executive Director and other necessary staff. The members of the Secretariat shall be either contracted directly or seconded by EITI Members.

2. The Secretariat shall be responsible for the day-to-day running of the EITI Association, including support to implementing countries, under the direction of the EITI Board through its Chair.

3. The Secretariat shall keep an updated Members' Registry at all times.

4. The Secretariat shall keep a record of these Articles of Association and any amendments thereto.

5. The Secretariat shall keep Minutes of all EITI Board Meetings, Members' Meetings and meetings of the EITI Conference in a Minute Book. All such Minutes shall be published on the EITI website. Such Minutes shall record the names of those present, the resolutions made at the meetings and, where appropriate, the reasons for the resolutions.

ARTICLE 16 THE EXECUTIVE DIRECTOR OF THE EITI SECRETARIAT

1. The Secretariat shall be led by a full-time Executive Director who will manage the day-to-day running of the EITI Association, including the selection of necessary staff, oversee development of the EITI Association and provide support to the EITI Board. The Executive Director shall report to EITI Board through the Chair and be responsible for the activities of the Secretariat.

2. The Executive Director, or their appointee from the Secretariat, shall serve as Secretary to all EITI Board Meetings, EITI Members' Meetings and EITI Conferences.

ARTICLE 17 FUNDING

1. The EITI Association is a non-profit association. Its funds consist of voluntary contributions from EITI contributors and grants from bilateral and multilateral donors, international financial institutions and other agencies, organisations and entities as determined by the EITI Board.

2. The EITI Association may also operate through voluntary contributions in kind.

ARTICLE 18 EITI ACCOUNTS, FUND MANAGEMENT AND PAYMENTS

1. The EITI Association holds a separate bank account in its own name, the "EITI International Management Account". The EITI International Management Account can be used for any activity falling within the objectives of the EITI Association and the work plans approved by the EITI Board. The funds may be applied to administration and governance costs, country-specific activities and multi-country activities.

2. The EITI Board shall appoint an external, independent auditor to annually audit the EITI International Management Account, and to present a written audit report to the EITI Board.

   The EITI Board shall develop reporting and auditing arrangements with respect to the EITI International Management Account which shall be set forth in the supplementary operating rules and procedures of the EITI Association.

ARTICLE 19 AMENDMENTS

1. These Articles of Association may be amended by the EITI Members' Meeting convened and held, pursuant to Article 8 by approval of at least two-thirds of the Members present.

   A proposal for an amendment shall be communicated in writing to all EITI Members four weeks in advance of the relevant resolution.

ARTICLE 20 REVIEW

1. A review of the governance arrangements of the EITI Association should be undertaken by the EITI Board within two years of the constitution of the Association.

ARTICLE 21 WITHDRAWAL AND DISSOLUTION

1. Any Member may withdraw from the EITI Association at any time. Such withdrawal shall become effective upon receipt of a written notification of withdrawal by the Executive Director.

2. The EITI Association may be dissolved by the Members' Meeting in accordance with the provisions of Article 8. A proposal for dissolution shall be communicated in writing to all EITI Members four weeks in advance of the relevant resolution.

3. In the event of a dissolution, the assets of the EITI Association shall be applied to similar objectives to those of the EITI Association and as determined by the EITI Board subject to the approval of the EITI Members' Meeting.

PH-695

ARTICLE 22 ENTRY INTO FORCE

1. These Articles of Association shall enter into force upon the constitution of the EITI Association.

ANNEX A The EITI Principles

As per section 1 in the EITI Standard.

ANNEX B Use of the EITI's name and logo

The EITI's name and logo are property of the EITI. As a general rule, use of the *EITI name*, i.e. EITI or Extractive Industries Transparency Initiative, by-products or translations, and *logo* or local derivatives, is encouraged and permitted under the limitations specified at https://eiti.org/logo-policy.

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-696

10. EITI Openness policy

1. **The documents of the EITI are public, except as otherwise provided below.**

2. Documents disclosed to the EITI on any matter concerning operational and/or business matters, which for **competition reasons** are important to keep secret in the interests of the person whom the information concerns, are exempted from access.

   For example, a business secret would normally be exempted if disclosure has the potential of influencing the competitive position of the company in question.

3. Documents revealing information received from a **third party are exempted from access if disclosure is likely to influence legitimate interests of that third party.**

   For example, access to documents will not be granted if the personal security of the third party and/or his family and/or any person closely connected to the third party in question may be endangered. Further, the protection of personal privacy will also qualify as legitimate interest and thus be exempted.

4. EITI **internal working documents** are exempted from access.

   For example, documents from the International Secretariat to the EITI Board and its Committees are normally considered internal documents and thus exempted. This exception applies if the International Secretariat, in the course of its preparation of a matter to the EITI Board, has prepared or commissioned an analysis or a report or the similar from an external source. In contrast, final minutes from the EITI Board meetings as well as committees and working group meetings are not internal documents. E-mails between EITI colleagues are normally considered to be internal working documents.

5. **Personal** information related to staff of the EITI is exempted from access.

   For example, documents on evaluations made in connection with recruitment and dismissal, and/or documents regarding assessments of staff performance and/or personal information about for example staff members' health are exempted from access. On the other hand, all contracts, salaries, compensation and expense accounting are public.

PH-697

11. EITI Constituency guidelines

The report of the International Advisory Group, as adopted by the Oslo Conference in October 2006, recommended that 'Each of the constituencies should agree how they wish to be represented on the proposed Board. This requires prior consideration by each constituency of how they define those eligible (i) to be selected as representatives; and (ii) to be involved in the selection process'.

The constituencies are defined in the EITI Articles of Association, which also determine the size of the constituencies' membership on the association and the number of seats on the EITI Board. Some of the EITI constituencies are informally sub-divided.

Updated guidelines for constituencies and sub-constituencies are available on the EITI website at eiti.org/governance.

PH-698

12. EITI Association code of conduct

1. Scope

All EITI Board Members, their alternates, Members of the EITI Association, secretariat staff (national and international), and members of multi-stakeholder groups (below referred to as "EITI Office Holders") shall abide by this Code of Conduct.

2. Personal behaviour, integrity and values

EITI Office Holders shall observe the highest standards of integrity and ethical conduct and shall act with honesty and propriety. The personal and professional conduct of EITI Office Holders should, at all times, command respect and confidence in their status as Office Holders of an association that promotes an international standard for transparency and accountability and should contribute to the good governance of the EITI.

EITI Office Holders should dedicate themselves to be leading by example and should represent the interests and mission of the EITI in good faith and with honesty, integrity, due diligence and reasonable competence in a manner that preserves and enhances public confidence in their integrity and the integrity of the EITI, and ensuring that his or her association with the EITI remains in good standing at all times.

3. Compliance

EITI Office Holders shall discharge their duties to the EITI in compliance with applicable national laws and regulations and with the EITI Rules, interests and objectives.

4. Respect for others

EITI Office Holders will respect the dignity, EITI-related needs and private lives of others and exercise proper authority and good judgment in their dealings with colleagues, members of the other EITI bodies, staff members, the general public and anyone whom they come in contact with during the discharge of their duties to the EITI.

5. Professionalism

EITI Office Holders should perform his or her assigned duties in a professional and timely manner and should use his or her best efforts to regularly participate in professional development activities.

PH-699

6. Discrimination

EITI Office Holders shall not engage in or facilitate any discriminatory or harassing behaviour directed toward anyone whom they come in contact with during the discharge of their duties to the EITI.

7. Confidentiality

EITI Office Holders shall not use any information that is provided in his or her role as EITI Office Holder and which is not already in the public domain in any manner other than in furtherance of his or her duties. EITI Office Holders continue to be bound by this obligation for two years after termination of their mandate.

8. Expenditure of EITI resources and use of EITI property

EITI Office Holders shall respect the principle of value-for-money and be responsible in the use of funds dedicated to the EITI. No EITI Office Holder shall misuse EITI property or resources and will at all times keep EITI property secure and not allow any person not appropriately authorised to have or use such property.

EITI Office Holders shall only bill at actual cost travel, operational or other costs related to the fulfilment of duty as an EITI Office Holder. EITI Office Holders shall provide goods or services to the EITI as a paid vendor to the EITI only after full disclosure to, and advance approval by the EITI Board or EITI multi-stakeholder group.

9. Conflict of interest and abuse of position

EITI Office Holders shall at all times act in the best interest of the EITI and not for interests such as personal and private benefits or financial enrichment.

EITI Office Holders shall avoid conflicts of private interest. For the purposes of this code, a conflict of interest is a situation or circumstance in which interests of EITI Office Holders influence or may influence the objective and impartial performance of their official EITI duties. In this regard, private interests include any advantage for themselves, their families or personal acquaintances.

EITI Office Holders finding themselves in such a situation must recuse themselves and inform the EITI Board or multi-stakeholder group of such recusal. For EITI Board Members the rules established in Article 5.6 of the EITI Articles of Association apply.

Specifically, EITI Office Holders shall follow these guidelines:

- Avoid placing (and avoid the appearance of placing) one's own self-interest or any third-party interest above that of the EITI; while the receipt of incidental personal or third-party benefit may necessarily flow from certain EITI-related activities, such benefit must be merely incidental to the primary benefit to the EITI and its purposes. Any per diems set, paid or obtained should be based on reasonable actual costs and good international practice[20].
- Refrain from overstepping the conferred powers. Office Holders shall not abuse EITI office by improperly using the EITI Association or the EITI's staff, services, equipment, resources, or property for personal or third-party gain or pleasure; EITI Office Holders shall not represent to third parties that their authority as an EITI Office Holder extends any further than that which it actually extends.
- Do not engage in any outside personal activities that could, directly or indirectly, materially adversely affect the EITI.

10. Gifts, trips and entertainment

EITI Office Holders shall not solicit or accept gifts, gratuities, free trips, honoraria, personal property, or any other item of value from any person or entity that are intended to be, or that can reasonably be perceived to be, a direct or indirect inducement to provide special treatment to such donor with respect to matters pertaining to the EITI.

Any offering or receiving of gifts, free trips or other compensation over the value of USD 100 directly or indirectly related to the discharge of EITI responsibilities should be declared to the EITI Board or the respective EITI multi-stakeholder group (through the international or national secretariats). Any offering or receiving of gifts considered excessive should be refused. In case of doubt whether a gift is excessive, the EITI Secretariat or multi-stakeholder group should be consulted. Should it be inappropriate to refuse an offering, notably because such refusal could prove embarrassing to the donor, the gift is to be surrendered to the EITI Secretariat or the multi-stakeholder group.

11. Implementation

The EITI Board, the respective EITI multi-stakeholder groups, the international or national secretariats are responsible for making EITI Office Holders familiar with this Code of Conduct and for providing advice and, if required, training on the interpretation and implementation thereof. Those, including EITI multi-stakeholder groups, responsible for making the EITI Office Holders familiar with this Code should annually confirm that EITI Office Holders are familiar with the Code and report on its implementation to the Board through the International Secretariat.

20 In establishing reasonable actual costs and good international practice, stakeholders may wish to consult the practices of the International Secretariat. When the Secretariat provides per diems (which it does not do to its staff), it often follows US Department of State's foreign per diem rates (https://aoprals.state.gov/content.asp?content_id=184&menu_id=78). In establishing per diems, national laws and regulations should of course be adhered to.

PH-701

12. Reporting

EITI Office Holders with a concern related to the interpretation, implementation or potential violation of this Code of Conduct shall bring such issues to the attention to the immediate EITI body. Where matters are brought to the attention of the EITI Board, the Board will consider the circumstances and consider whether action is necessary in accordance with the EITI Principles, the EITI Standard and the Articles of Association. Anybody who is uncomfortable to raise any such concerns with the immediate EITI body may bring their concerns to the attention to the EITI Board through its Governance Committee and its chair.

COMMISSION OF INQUIRY INTO STATE CAPTURE

COMMISSION OF INQUIRY
INTO STATE CAPTURE

PH-703

Guided by the belief that a country's natural resources belong to its citizens, the EITI has established a **global standard** to promote the open and accountable management of oil, gas and mineral resources.

The EITI Standard requires the disclosure of information along the extractive industry value chain, from how extraction rights are awarded, to how revenues are managed and allocated by government.

By doing so, the EITI seeks to foster multi-stakeholder collaboration, promoting a healthier and more accountable sector that can play a positive role in development.

Extractive Industries Transparency Initiative

eiti.org

PH-704

Clear signal to foreign investors: Hasty go ahead for Guptas to buy Optimum

23rd February 2016 by Alec Hogg

PH-705

Regulatory inconsistency has wrought great damage on the South African economy. Among the perpetrators has been the Competition Commission which often adopted a politically-motivated approach, distorting the overriding brief of promoting greater competition in the economy. But just when when you hoped there would be consistent inconsistency, there's none. Despite concerns around backroom shenanigans and Gupta strong-arming of mining multinational Glencore, this time the Competition Commission stuck to a tight brief. It has moved rapidly to flick the green light on a deal that shouts out for detailed investigation. By so doing, a clear signal is sent to foreign investors. One reinforcing perceptions that in South Africa nowadays, political influence trumps foreign investment. – Alec Hogg

By Dane McDonald and Matthew le Cordeur

Cape Town – The Competition Tribunal on Monday approved the controversial merger between the Tegeta Exploration and Resources, whose shareholders include President Jacob Zuma's son and the Gupta family, and Optimum Coal Mine.

Tegeta agreed to buy Optimum for R2.15bn in December 2015 after Glencore had placed the mine under administration because it said it couldn't make a profit because of the terms of a coal supply deal with Eskom.

PH-706

According to a Bloomberg report Tegeta is 64% owned by by Mabengela Investments, which in turn is 45% owned by Duduzane Zuma. Tegeta is a joint venture between the latter and the Guptas' Oakbay Investments.

The merger was approved with a condition that prohibited "merger specific retrenchments" and imposed a set of "monitoring conditions" on the parties.

Aside from employment concerns the Commission found that the merger was unlikely to lessen competition in the market "as they were relatively small players when compared with rivals such as Anglo American and Exxaro Coal".

> Read also: How world sees SA: Guptas pulled levers of State to grab Glencore's Optimum

PH-707

Tegeta will supply coal to three Eskom power plants: Hendrina, Komati and Majuba.

The Optimum Coal Mine sale has thrust Eskom's coal contracts into the spotlight.

The Guptas are increasingly making headlines due to deals that are linked to Duduzane and their perceived influence over the president.

The recent headlines include its arms contract with state-owned company Denel, influence over cabinet appointees Mosebenzi Zwane (mines minister) and Des van Rooyen (finance and Cogta), its sponsorship of the SABC breakfast show and recent coal deals.

It was reported this weekend that Gordhan would not partake in the New Age Breakfast show on SABC after his budget speech this Thursday.

The New Age is a newspaper owned by the Guptas, which does not share its circulation publicly, but is circulated in government departments and state-owned entities.

Molefe's surprise comes as Eskom has already started this process with Treasury, Eskom said.

> Read also: James Lorimer: Optimum's loss, Guptas gain, Private profiteering from SOEs.

It submitted contracts to Treasury for coal and diesel including a register of payments made to various suppliers in 2015 after a request from the department on June 25 2015, Eskom said.

It said Treasury visited Eskom's head office on July 23 2015 to clarify certain information they needed, and to also get additional documents which could not

PH-708

sent electronically because of their size.

Treasury's last request for additional information from Eskom was on October 21 2015, which was duly submitted, said Eskom.

Eskom said it has demonstrated a serious commitment to deal with corruption and maladministration issues. – Fin24

Source: http://www.fin24.com/Companies/Mining/tegeta-optimum-merger-approved-with-condition-20160222

Share This Post

Sponsored Content

Cheap Wireless Earphones Everyone in South Africa is Talking

techgadgetdiscounts.com

Born Between 1954 and 2000? You Might Be Eligible For This New

Experts In Money Insurance

New Groundbreaking Technology Makes Landlines Obsolete -

VoIP | Sponsored Listings

Top 19 Black Friday Deals That You Can Already Claim In South

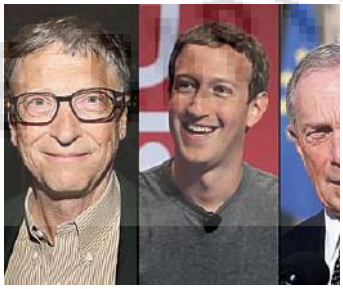
Black Friday Deals Guide

Most Daring Dresses at the 2019 Academy Awards

Family Minded

Geography Facts That Will Blow Your Mind

Far and Wide



Where Do The Richest Americans Live?

Mansion Global

European Countries, Ranked from Worst to First

Far and Wide

Recommended by

Cyril Ramaphosa: The Audio Biography

Listen to the story of Cyril Ramaphosa's rise to presidential power, narrated by our very own Alec Hogg.

Get the Audiobook

Narration by Alec Hogg

Comments Community 1 Login

Recommend Tweet Share Sort by Best

Join the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name

vramaarnet • 4 years ago

Why, if a company that specialises in mining could not make money with the terms of the Eskom supply deal, can the Zuma/Gupta company make money? Or will the terms now be more favourable? Is the Competition Commission not also shown up to be a bunch of stooges carrying out whatever is favourable to the corrupt Zuma?

2 • Reply • Share ›

peterq ↳ vramaarnet • 4 years ago

Eskom helped by bankrupting the company by lowering the price they would pay for the coal, so the Guptas could "buy" it. The Guptas will then get about 4x more then other suppliers. The Guptas will make the money because they did not pay for it, the IDC paid for them, then as stated they will get a much better price. They can and will go back to the IDC for a top-up. Then they also have SARS in their pocket, so do not expect them to pay too much tax. A great money spinner.

1 • Reply • Share ›

PH-710

Pieter peterq • 4 years ago

Exactly, price difference something like R140/ton to Glencore and R500 per ton to Guptas. Somebody in Eskom must also get shares because they ensured that the mine were bankrupted.

Off topic but I sometimes wonder if that is not what is happening on a larger scale with the country. A country like example China can pay a moron like Julius R10 mil per month to cause havoc and publicly make stupid remarks. That damage the currency and cause businesses to close. China buy resources at 40% discount because of poor currency and they can come and buy failed businesses at a fraction of the cost.

1 • Reply • Share ›

Danny Harris Pieter • 4 years ago

Thats my theory too. As an older South African I remember many occassions when we were warned of the communist threat. That threat has never gone away and I suspect that China understood the weak nature and character of the average African politician and you only have to look northwards for evidence. This is also why there will never be an African renaissance. What is not quite right with this theory is that the rest of the western world must understand the threat that if China has a stranglehold on the the raw materials of Africa that it could also dominate and clearly they helped that to happen. Hmmm!

• Reply • Share ›

vramaarnet peterq • 4 years ago

If peterq has this information why not publish it chapter and verse with supporting documentation? That way what peterq knows is available to the authorities and it becomes incumbent upon them to enforce the law.

• Reply • Share ›

Ace • 4 years ago

South Africa is now firmly established as a corrupt state.
Its very sad.

1 • Reply • Share ›

John Dove • 4 years ago • edited

Can anyone name another deal of this size on which the Competition Commission ruled in two months (which

Popular Posts

Retire at 55 and live to 80; work till you're 65 and die at 67. Startling new da...

You are foolish to believe the 'lies' about the DA - Frans Cronjé

How the going got weird at Independent – by the not-so-weird who went

SAA to chop jobs; Impala eyes Zim deal; Saldanha Steel closes; Facebook fake ads...

France mulls Eskom aid; Loadshedding dents rand surge; Branson considers SAA sta...

Biznews Radio

Biznews Radio

Independent Media liquidation looms; unions battle

00:00 / 05:11

Biznews Radio

Subscribe to podcast

Welcome to BizNews Radio where we interview top thought leaders and businesspeople from South Africa and across t...

Independent Media liquidation looms; unions battle SAA, govt over job cuts; world's richest move... 05:11
Sekunjalo Independent Media on Tuesday received an application for its liquidation from the Public In... Nov 12

SAA to chop jobs; Allan Gray dies; Impala eyes Zim deal; Saldanha Steel closes; Facebook fake ads;... 05:46
South African Airways, the beleaguered state-owned airline that's reliant on government financial supp... Nov 11

France mulls Eskom aid; Loadshedding dents rand surge; Branson considers SAA stake 05:10
In today's business headlines: France is considering providing financial support to Eskom according to ... Nov 10

Moody's next move: What's next for SA; Shoprite, Dischem, Multichoice, wine markets 04:55
Most analysts following South Africa expect it to lose its final investment-grade rating. But they disagree... Nov 7

SA attracts $16bn; Hurry up and fix Eskom, investors urge govt; 2020 EM outlook; Intu plunges 04:38

Get Daily Updates

Subscribe to our Newsletter to get daily updates on local affairs, with a global context.

First Name

Last Name

Email Address *

Get Daily Updates

Visit the BizNews Shop

The BizNews Shop

Everything from investing like Warren Buffett to the Audiobiography of Cyril Ramaphosa.

Visit the Shop

Biznews LIVE

BizNews

Biznews Radio

All Business 24/7

Surveillance Special: Schwarzman On "What It Takes"
Bloomberg Radio
Bloomberg Surveillance
23:05

Powered by SAM

BizNews

Company

About BizNews

How To Support BizNews

Make us your Homepage

Contact BizNews Support

Advertisers

Advertising on BizNews

Sponsored Content Disclaimer

BizNews Premium

BizNews Premium

Biznews Premium FAQs

Login

Newsletter

First Name

Last Name

Email Address *

Get Daily Updates

© 2019 BizNews, Inc. | The Rational Perspective Terms & Conditions Comments Policy

COMMISSION OF INQUIRY INTO STATE CAPTURE

Prevention and Combating of Corrupt Activities (Act No. 12 of 2004)

(South African Legislation)

PH-718

REUTERS

UK

OCTOBER 10, 2018 / 1:12 PM / A YEAR AGO

Azeri banker's high-spending wife targeted by new British anti-graft powers

Michael Holden, Andrew MacAskill

LONDON (Reuters) - The first target of new British powers to combat the proceeds of suspected corruption is the wife of a jailed Azeri banker who spent more than 16 million pounds at luxury department store Harrods, London's High Court has revealed.

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-719

A sale sign is seen at dawn on the outside of the Harrods store in Knightsbridge in London, January 5, 2018. REUTERS/Toby Melville

An anonymity order was lifted after Zamira Hajiyeva, the wife of the former chairman of Azerbaijan's largest bank, last week lost an appeal against an attempt by authorities to seize a property and a golf course worth about 22 million pounds.

This is the first time British authorities have used an Unexplained Wealth Order (UWO), a power which came into effect earlier this year and aims to force foreign officials suspected of corruption and their families to account for their wealth.

Police say about 100 billion pounds of dirty cash moves through or into Britain each year, buying everything from luxury London homes to whole companies. They say they are focused on cracking down in particular on money from Russia, Nigeria, former Soviet states and Asia.

When a UWO is used the onus is on the owner to show that any asset worth more than 50,000 pounds was obtained legitimately.

Hajiyeva's husband Jahangir Hajiyev, who was chairman of state-owned International Bank of Azerbaijan (IBA) from 2001 to 2015, was convicted by an Azeri court in 2016 of fraud and embezzlement and sentenced to 15 years in jail.

The Azeri finance ministry said about $3 billion could have been misappropriated by Hajiyev, who denied the charges.

Lawyers for Hajiyeva, who denies any wrongdoing, said that Hajiyev was convicted after a show trial and the circumstances of the case did not meet UWO requirements. They did not respond to requests for comment, but have previously said they would take the case to London's Court of Appeal.

Britain's National Crime Agency (NCA) successfully applied for orders against Hajiyeva demanding she reveal the source of her wealth or risk losing the properties.

One order covers a home in London's Knightsbridge, about 100 metres from Harrods, which was bought for 11.5 million pounds by a company registered in the British Virgin Islands. The other order concerns Mill Ride Golf Club in Ascot, west of London.

PH-720

Last week, judge Michael Supperstone rejected Hajiyeva's appeal against one of the UWOs. Supperstone also ruled that Hajiyeva's name, which previously could not be disclosed, could be made public on Wednesday.

MAN OF MEANS

The NCA had alleged Hajiyeva bought two properties using money embezzled by her husband when he worked for the IBA.

Hajiyeva said in a witness statement that her husband was a man of substantial means. Supperstone's written ruling made reference to a document prepared by Werner Capital from 2011 which stated his net worth to be about $72 million.

Hajiyeva spent 16.3 million pounds ($21.3 million) under a loyalty card scheme at Harrods between 2006 and 2016, using 35 credit cards issued to her by the IBA.

She spent 121,000 pounds at Harrods on a single day, buying unidentified goods from luxury jewellery, perfume and watch brand Boucheron and two weeks earlier splashed out 48,600 pounds on an item from Cartier, court documents show.

However, letters from the bank showed Hajiyev's net income from IBA was just $29,062 in 2001, rising to $70,648 in 2008.

"Where we cannot determine a legitimate source for the funds used to purchase assets and prime property, it is absolutely right that we ask probing questions to uncover their origin," said Donald Toon, the NCA director for economic crime.

"Unexplained Wealth Orders have the potential to significantly reduce the appeal of the UK as a destination for illicit income," Toon said.

Additional reporting by Margarita Antidze in Tbilisi; editing by Stephen Addison and Alexander Smith

Our Standards: The Thomson Reuters Trust Principles.

PH-721

PAID PROMOTIONAL LINKS

Promoted by Dianomi

Gain new perspective. Learn how to turn your career into your calling.

HBS Executive Education

Learn how to think differently, innovate, and be a game-changer. Go.

HBS Executive Education

Build the skills you need to thrive in fast-changing industries. Go.

HBS Executive Education

Do you have the hard and soft skills it takes to succeed in new roles?

HBS Executive Education

Going Green

The AIC

PH-722

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-723

MORE FROM REUTERS

Merkel expects British parliament to approve Brexit deal

12 Nov

Hackers hit UK political parties with back-to-back cyberattacks

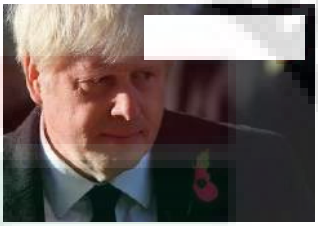
12 Nov

Brexit Party leader Farage snubs calls not to contest Labour seats

12 Nov

EU pushes Brexit Britain to name new commissioner

12 Nov



Conservatives' lead over Labour narrows slightly - Survation poll

12 Nov

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-724

COMMISSION OF INQUIRY INTO STATE CAPTURE

PH-725

MORE FROM REUTERS

Sterling is my idol and England leader, says Hudson-Odoi

12 Nov

UK jobs fall by most in over four years as election nears

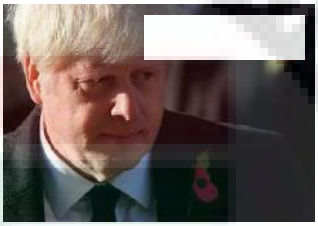
12 Nov

HSBC and RBS set to launch new digital banking platforms

11 Nov

Hong Kong universities become 'battlefields' as citywide violence...

13 Nov



Conservatives' lead over Labour widens slightly - ICM poll

11 Nov

COMMISSION OF INQUIRY INTO STATE CAPTURE

Apps Newsletters Advertise with Us Advertising Guidelines Cookies Terms of Use Privacy

All quotes delayed a minimum of 15 minutes. See here for a complete list of exchanges and delays.

© 2019 Reuters. All Rights Reserved.

PH-727

Home Office

Requests for Mutual Legal Assistance in Criminal Matters

Guidelines for Authorities Outside of the United Kingdom - 2015

12th Edition

International Criminality Unit, Home Office, 3rd Floor Seacole Building, 2 Marsham Street, London SW1P 4DF
mlapolicy@homeoffice.gsi.gov.uk
March 2015

CONTENTS

SECTION 1: Introduction 4
Role of Central Authorities in the UK 4
Requests for the Crown Dependencies and UK Overseas Territories 5
Types of Assistance 5
International Agreements 5
Reciprocity 6
Confidentiality 6
Collateral Use - Requests Made by the UK 6
Collateral Use - Requests Made to the UK 6
Law Enforcement (Police) Cooperation 7

SECTION 2: How to Make a Request 8
Is MLA Appropriate? 8
Who Can Send an MLA Request 8
De Minimis Requests 8
Dual Criminality 9
Language of Requests 9
Format of a Request 9
Transmission 11
Where to Send MLA Requests 11
Timescales 13
Queries about Requests 13
Urgent Requests 14
Cost of Executing Requests 14
Notification Where Assistance is No Longer Required 14
Linked Requests 14
Refusal of MLA Requests 15

SECTION 3: Types of Assistance 16
Service of Process 16
Statements and Interviews 18
Evidence on Oath/in Court 19
Hearings via Video or Telephone Conference 21
Asset Tracing 23
Production Orders 24
Search and Seizure 26
Communications Data 28
Live Interception of Communications 30
Restraint (Freezing) 31
EU Freezing Order 35
Confiscation & Forfeiture 36
EU Confiscation Order 39
Temporary Transfer of a Prisoner for Purposes of Investigation 40
Passport Information and Immigration Status 43
Transfer of Proceedings 44
Criminal Records 46
Judicial Records 47
Other Requests for MLA 50

PH-729

SECTION 4: Foreign Officers in the UK 53

SECTION 5: Civil Matters 54

Civil Forfeiture of Assets..... 55

COMMISSION OF INQUIRY INTO STATE CAPTURE

SECTION 1: Introduction

Mutual Legal Assistance (MLA) is a method of cooperation between States for obtaining assistance in the investigation or prosecution of criminal offences. MLA is generally used for obtaining material that cannot be obtained on a law enforcement (police to police) to basis, particularly enquiries that require coercive means. Requests are made by a formal international Letter of Request (ILOR or LOR). In civil law jurisdictions these are also referred to as *Commissions Rogatoires*. This assistance is usually requested by courts or prosecutors and is therefore also referred to as 'judicial cooperation'.

MLA can also be used to obtain assistance in the investigation of the proceeds of crime and also in their freezing and confiscation. Proceeds of crime matters can be on a criminal (conviction) basis or a civil (non conviction) basis.

Due to the increasingly global nature of crime, MLA is critical to criminal investigations and proceedings both in the UK and abroad. The UK is committed to assisting investigative, prosecuting and judicial authorities in combating international crime and is able to provide a wide range of MLA. MLA is also a vital tool in the pursuit of criminal finances including the recovery of the proceeds of crime that may have been moved and hidden assets overseas.

These guidelines are to ensure that requests for MLA received by the UK can be acceded to and executed quickly and efficiently. The guidelines include:

- Guidance to authorities who wish to make a **formal request for MLA** to the UK ('requesting authorities');
- Guidance to authorities on what can be requested **without** making a formal request for MLA to the UK;

These guidelines contain advice on how to make an MLA request, service of process, transfer of proceedings, and restraint and confiscation of property.

Role of Central Authorities in the UK

Central authorities have the function of receiving, acceding to and ensuring the execution of MLA requests. Subject to the exceptions below, all formal requests for assistance **must** be sent to a central authority for consideration. The UK has three central authorities:

- Home Office UK Central Authority ('UKCA) for MLA requests in England, Wales and Northern Ireland;
- Her Majesty's Revenue and Customs ('HMRC') for MLA requests in England, Wales and Northern Ireland relating to tax and fiscal customs matters only, for example, the collection and management of revenue, the payment of tax credits;
- Crown Office for MLA requests in Scotland (including devolved Scottish tax matters).

The following are exceptions to when to using a central authority to receive requests:

- EU Freezing Orders for property must be sent to the relevant UK prosecuting authority for the purposes of recognition and execution (except "property related to terrorism offences or investigations" which must be sent to a central authority);
- EU Confiscation Orders must be sent to the relevant UK prosecuting authority for the purposes of recognition and execution.

Contact details for all relevant UK authorities are in Section 2.

Requests for the Crown Dependencies and UK Overseas Territories

The Crown Dependencies (Bailiwicks' of Guernsey and Jersey, and the Isle of Man), and the UK Overseas Territories (Anguilla, Bermuda, British Virgin Islands, Cayman Islands, Falklands, Gibraltar, Montserrat, St Helena, Turks and Caicos Islands, and Pitcairn) are not part of the UK.

The Crown Dependencies and the Overseas Territories are wholly responsible for executing requests within their own jurisdictions.

MLA requests for the Crown Dependencies and the Overseas Territories must not be sent to the UK.

MLA requests should usually be sent to the Attorney General of the Crown Dependency or Overseas Territory from where the assistance is required. The contact details for these jurisdictions can be found here.

Requests for intelligence from the Crown Dependencies, Falklands, and St Helena should be submitted via the National Crime Agency (NCA). The other Overseas Territories host Interpol sub-bureaux.

Types of Assistance

There is a wide range of MLA that can be provided by the UK conditional on the correct criteria being met. Please refer to Section 3 of this guide for information about the most common types of MLA.

In some cases evidence can be obtained via law enforcement cooperation'. Where such cooperation is available for a specific measure this is highlighted in Section 3.

International Agreements

The UK is party to a number of bilateral and multilateral MLA treaties (see this link for a list of the international agreements that the UK is party to). The UK can provide MLA to any country or territory in the world, whether or not that country is able to assist the UK, and whether or not there is a bilateral or multilateral agreement. However where an agreement imposes specific conditions or procedures, the UK expects these to be adhered to.

The European Investigation Order ('EIO') is a European directive aimed at streamlining the process for MLA between participating EU Member States. It will introduce deadlines and

PH-732

standardised EIO forms for requesting assistance. The directive entered into force on 22 May 2014 and will be implemented in the UK in May 2017. The UK will not accept EIOs until implementation in 2017.

Reciprocity

The UK does not generally require reciprocity but would expect assistance from countries which are parties to relevant bilateral or international agreements with the UK. The UK would also expect reciprocity from countries to which we give assistance without a treaty or an international agreement. Reciprocity is required in all requests for assistance in tax matters.

Confidentiality

It is usual policy for central or executing authorities to neither confirm nor deny the existence of an MLA request, nor disclose any of its content outside government departments, agencies, the courts or enforcement agencies in the UK without the consent of the requesting authority, except where disclosure is necessary to obtain the co-operation of the witness or other person concerned.

Where public statements are made by an overseas authority about the assistance it is requesting from the UK, the central authority should be notified so that they may respond appropriately to any media or public enquiries.

In general, requests are not shown or copied to any witness or other person, nor is any witness informed of the identity of any other witness. In the event that confidentiality requirements make execution of a request difficult or impossible, the central authority will consult the requesting authorities. In cases where disclosure of a request or part thereof is required by UK domestic law in order to execute the request, it will normally be the case that the requesting authority will be given the opportunity to withdraw the request before disclosure to third parties is made.

From time to time the Home Office releases statistical data on the number of MLA requests sent and received. Such data is only released where to do so would not breach the confidentiality of any individual request. See this link for published data.

Collateral Use - Requests Made by the UK

Evidence obtained **by the UK** pursuant to an MLA request to a foreign authority will not be used for any purpose other than that specified in the original request without the consent of appropriate overseas authority (see section 9(2) of Crime (International Co-operation) Act 2003 ('CICA') and also the Court of Appeal decision of Crown Prosecution Service & Anor v Gohil [2012]).*"*

Collateral Use - Requests Made to the UK

Where a requesting authority wishes to use evidence obtained **from the UK** for a different purpose to that stated in the original MLA request, or to share the evidence with a third country, a formal request to do so must be made in writing by the original requesting state to the relevant

PH-733

central authority in the UK (unless otherwise stated in a relevant treaty). The additional request must contain the following information:

Request to Use Evidence for other Purposes
✓ The central authority's reference number for the original request;
✓ What evidence is to be used/shared;
✓ How this evidence will be used/shared;
✓ Why this evidence is needed in this new/other investigation / court proceedings.

Law Enforcement (Police) Cooperation

This entails police and other law enforcement officers in a requesting state asking for the assistance of law enforcement agencies in the UK to gather information for an investigation. This can be an easier and quicker way to obtain intelligence and evidence, as it does not require a request. In many countries' legal systems, information collected by UK law enforcement agencies is directly admissible as evidence in criminal trials abroad (with the permission of UK law enforcement). For instance countries which do not require evidence to be sworn by witnesses in a court under their domestic law can consider using law enforcement cooperation to request information to be used as evidence.

If direct contact between a foreign police force and a UK police force has not already been established, the NCA should be contacted with the request. The NCA acts as the UK Interpol gateway for all incoming and outgoing police enquiries. The NCA will forward requests through the Interpol network to the relevant police force or other law enforcement agency who will then execute the request, subject to any data sharing agreement.

The following UK law enforcement agencies can receive enquiries directly from law enforcement officers in foreign jurisdictions (in some cases this will be subject to a data sharing agreement or memorandum of understanding):

- UK Liaison Bureau at Europol via the NCA;
- Interpol via NCA;
- UK Visas & Immigration;
- HMRC;
- Police Services;
- Financial Intelligence Units;
- Asset Recovery Offices.

Back to Contents

PH-734

SECTION 2: How to Make a Request

Requests for MLA must be sent to the relevant central authority, unless they are requests for service of process or mutual recognition of a freezing or confiscation order.

Requests which do not comply with the requirements set out below may be returned to the requesting authority and may not be executed.

Is MLA Appropriate?

In some cases a MLA request is not suitable because:

- The material can be obtained **voluntarily** without any assistance from UK authorities (although UK law enforcement should be notified);
- The material can be obtained via **law enforcement cooperation** (see above) because it is only required for intelligence purposes or material obtained in this way is admissible as evidence.

It is often desirable for overseas authorities to obtain intelligence prior to making an MLA request. This can help improve the quality of the MLA request, and makes it less likely that a request will be returned to the requesting authority for lack of information.

Requests for assistance in **civil matters** are dealt with by a different process, as explained in Section 5 of this guidance.

Who Can Send an MLA Request

Any competent body under the law of the requesting country may issue a request to the UK. This includes a court exercising criminal jurisdiction or a prosecuting authority outside the UK.

De Minimis Requests

UK executing authorities have limited public resources available, and *de minimis* (trivial or disproportionate) MLA requests may be refused by the Home Office on these grounds if they meet the criteria (or comparable criteria) set out below.

De Minimis Requests	
✓	There has been a financial loss or gain or damage of less than **£1,000**; or
✓	The alleged offence was committed more than **10** years ago (and there is no, or insufficient, explanation for the delay in investigation or prosecution).

PH-735

When considering the criteria the following factors are also taken into account:

- Whether there are any aggravating factors;
- Whether a UK prosecuting authority would send a request in similar circumstances;
- Whether the request is for a 'coercive' measure;
- Whether there are resource implications for a number of executing authorities.

Please note that Scotland and HMRC do not apply a *de minimis* policy.

Dual Criminality

The UK generally only requires dual criminality for search and seizure, production orders (including banking evidence), and restraint and confiscation. A *'conduct'* based approach is taken, i.e. the conduct underlying the alleged offence is considered when assessing dual criminality, rather than seeking to match the exact same term or offence category in both jurisdictions.

Failure to pay child maintenance is not a criminal offence in the UK. The UK cannot use any investigative measure which requires dual criminality to provide the evidence requested. As an alternative to MLA evidence can also be obtained using civil routes (see below) and EU Member States may seek enforcement through Council Regulation No 4/2009.

Language of Requests

All requests should be in English. If an English translation is not provided, is incomplete, or is not carried out to a high professional standard, the request will be sent back to the requesting authority.

Format of a Request

Requests must always be made in writing. A request can be sent electronically (e.g. in a 'pdf' format via email), but an original hardcopy may be requested.

Information to be Included in a Request
✓ Headed notepaper of the issuing authority must be used;
✓ Details of the authority making the request, including the name, telephone number and email address (where available) of a contact person;
✓ For requests not made in the English language; one signed version of the non-English request **and** one translation of the request into English.
✓ The original request must be signed by the issuing authority;
✓ Purpose for which assistance is sought;

- ✓ The type of assistance requested and any additional information that is required for requests for this type of assistance (see Section 3 of these guidelines);
- ✓ A description of the offences charged or under investigation and sentence or penalty;
- ✓ A copy of the legislation that criminalises the conduct in the requesting country and gives information on the offence, penalty and rights a person may be afforded;
- ✓ A summary of the facts giving rise to the request and connection to the UK;
- ✓ Details of the person or persons (including legal persons) named in the request including, where available, address/location, date of birth and nationality (*if confidential this can be sent separately to the request*);
- ✓ Whether the person(s) named in the request are witnesses, suspects or victims;
- ✓ Whether the evidence requested is exculpatory;
- ✓ The connection between the evidence requested and the offence under investigation or proceedings. A clear *nexus* must be established. This goes further than just stating that the requested material is relevant to the case.
- ✓ Relevant dates e.g. date of court hearing (reason for special urgency or attention should be included in the covering letter of request);
- ✓ Details, including the telephone number and e-mail address if available, of any UK law enforcement agency or officers who are familiar with the investigation (including, if relevant, the names of UK based operations which the requesting authority is aware of);
- ✓ If applicable, the title of the relevant convention or bilateral treaty under which the request is being made (please see this link for conventions and treaties the UK is party to);
- ✓ If applicable, details of any media attention, sensitivities or reasons for high profile interest in the case;
- ✓ If the death sentence is a possible sentence or penalty for the offence under investigation, an assurance that such a sentence will not be carried out or will be commuted;
- ✓ If applicable, the reference numbers of any linked requests.

Failure to provide the fullest information possible may result in delays or in a request not being executed in whole or in part. Please see our website for example request templates.

PH-737

Transmission

The UK does not require requests to come via diplomatic channels and central authorities are content to receive requests directly. However, the requesting authority will need to comply with its own domestic laws relating to the transmission of requests. Requests to:

- Home Office can be sent requests via post / courier or fax/email;
- HMRC can be sent via post or email;
- Crown Office can be sent via post, email, courier or fax.

EU Freezing/Confiscation orders for property can be sent to the PPSNI, CPS, SFO via post/courier or fax/email.

Please note that email transmission of requests is not secure.

Procedural documents can be served on affected individuals directly by post. Please see further details on this in Section 3

Where to Send MLA Requests

England & Wales and Northern Ireland Should Be Directed To:	
UK Central Authority International Criminality Unit Home Office 3rd Floor Seacole Building 2 Marsham Street London SW1P 4DF *For requests for civil forfeiture see section 5*	Fax: +44 20 7035 6985 Tel: +44 20 7035 4040 Email: UKCA-ILOR@homeoffice.gsi.gov.uk

Scotland Should Be Directed To:	
International Co-operation Unit Crown Office 25 Chambers Street Edinburgh EH1 1LA	Tel: +44 131 243 8152 Fax: +44 131 243 8153 Email: coicu@copfs.gsi.gov.uk

PH-738

Tax and Fiscal Customs Matters In England & Wales and Northern Ireland Should Be Directed To:	
Criminal Law Advisory Team HM Revenue and Customs Solicitor's Office Room 2E/10 100 Parliament Street London SW1A 2BQ	Fax: +44 207 147 0433 Email: mla@hmrc.gsi.gov.uk

Crown Dependency or Overseas Territory Should Be Directed To:
The relevant authority listed at this link.

Orders to freeze or confiscate property (except terrorist property) under Council Framework Decision 2003/577/JHA or Council Framework Decision 2006/783/JHA must be sent to the relevant **prosecuting authority** in the UK. Orders to freeze evidence or terrorist property must be sent to the relevant central authority (above).

Orders to freeze or confiscate property in England & Wales under Council Framework Decision 2003/577/JHA or Council Framework Decision 2006/783/JHA:	
Crown Prosecution Service Proceeds of Crime Rose Court 2 Southwark Bridge London SE1 9HS For complex fraud, bribery and corruption cases: Serious Fraud Office (SFO) Proceeds of Crime Serious Fraud Office 2–4 Cockspur Street London SW1Y 5BS	

Orders to freeze or confiscate property in Scotland under Council Framework Decision 2003/577/JHA or Council Framework Decision 2006/783/JHA:	
International Co-operation Unit Crown Office 25 Chambers Street Edinburgh EH1 1LA	Tel: +44 131 243 8152 Fax: +44 131 243 8153 Email: coicu@copfs.gsi.gov.uk

Orders to freeze or confiscate property in Northern Ireland under Council Framework Decision 2003/577/JHA or Council Framework Decision 2006/783/JHA:	
Public Prosecution Service for Northern Ireland (PPSNI) High Court & International Section Belfast Chambers 93 Chichester Street Belfast BT1 3JR	

Timescales

The Home Office will consider an MLA request within 30 days of receipt, and the Crown Office within three working days. However, depending on the nature of the request this may not always be possible. All central authorities will take into account any reasons for urgency which are clearly stated in the request. Failure to follow the advice in these guidelines may also delay the acceptance and execution of the request.

Queries about Requests

Once a central authority has received a request for MLA the request will be logged and given a reference number. In England, Wales and Northern Ireland a caseworker will be assigned to the case. HMRC handle these requests centrally within their team. In Scotland the case will be allocated to a Procurator Fiscal Depute (Scottish Prosecutor).

The requesting authority will be written to with the details of the person dealing with their case. Any subsequent correspondence relating to the MLA request should be sent to the correct caseworker/ HMRC team/ Procurator Fiscal Depute and should always quote the central authority's reference number.

PH-740

Urgent Requests

If a request is urgent the central authority will try to deal with the request as quickly as possible.

Urgent Requests
✓ **Do not mark a request as urgent unless it is urgent;**
✓ Detail why a request is urgent, for example: somebody is being detained in custody; somebody is due to be released from custody; pre-trial court appearances or trial dates; there is an immediate risk to individuals; risk of dissipation of assets etc;
✓ Provide the dates of any deadlines which need to be met.

Cost of Executing Requests

Ordinarily the UK will meet the costs of executing a request. Exceptions include:

- fees and reasonable expenses of expert witnesses;
- the costs of establishing and operating video-conferencing or television links in England, Wales and Northern Ireland (Scotland does not charge for television links), and the interpretation and transcription of such proceedings;
- costs of transferring persons in custody;
- costs of obtaining transcripts of proceedings and judges' sentencing remarks; and
- costs of an extraordinary nature agreed with the requesting authority (these will be agreed before costs are incurred);
- costs of legal representation during a suspect interview where the requesting authority states that a defence lawyer must be present.

Notification Where Assistance is No Longer Required

Should the requested assistance no longer be required, the central authority should be informed immediately, quoting the central authority reference number.

Linked Requests

Requests which relate to a previous request can be sent to the central authority as a linked (including supplementary) request.

Information to Include in a Linked Request
✓ A statement that this request is linked to a previous request;
✓ the central authority's reference number for the previous request;

✓ All the information relevant to a standard MLA request (see above), plus any further information relating to the specific type of additional request.

Refusal of MLA Requests

In practice the UK accedes to most requests received and in general there is a presumption that MLA will be provided where all the requirements of the investigative measure under UK law have been met. However, the central authorities retain a wide discretion when considering whether to accede to a request.

Possible Grounds for Refusal Include:
✓ The request relates to an investigation or prosecution which is politically motivated;
✓ The execution of the request would prejudice the sovereignty, security or other essential interests of the UK;
✓ The execution of the request would prejudice the *ordre public* of the UK (this includes the risk that the death penalty will be imposed for the crime under investigation);
✓ The request is *de minimis;*
✓ The request relates to a person who, if proceeded against in the UK for the offence for which assistance is requested, would be entitled to be discharged on the grounds of a previous acquittal or conviction (double jeopardy);
✓ The request relates to an offence that the UK regards as an offence under military law, which is not also an offence under ordinary criminal law;
✓ There are substantial grounds for believing that the request has been made for the purpose of investigating, prosecuting or punishing a person on account of his/her race, gender, sexual orientation, religion, nationality, ethnic origin or political opinions or that person's position may be prejudiced for any of those reasons;
✓ The request is for a coercive or intrusive measure for which the UK requires dual criminality and in respect of which there is no equivalent UK offence.

Further information on how the UK considers human rights issues in the context of the provision of assistance can be found in the Overseas Security & Justice Assistance (OSJA) guidance.

Back to Contents

SECTION 3: Types of Assistance

This section details the forms of assistance the UK can provide and the specific information which should be included in requests.

Service of Process

Procedural documents may be sent **directly** by the requesting authority to the persons in the UK to whom they relate. The UK strongly encourages direct transmission of procedural documents to persons by post, unless this is not legally possible under the domestic law of the requesting authority.

Under Article 5 of the EU Mutual Assistance Convention 2000 (MLAC), EU Member States must send procedural documents directly to the person concerned, unless one of the reasons in Article 5(2) applies. Failure to do so may result in the request being returned to the requesting authority.

Service via a Central Authority

In line with sections 1 and 2 of CICA, a request may be made to the Home Office or the Crown Office for the service of procedural documents (e.g. a summons or judgment) issued by a court or authority in the requesting state in relation to criminal proceedings. HMRC is not a central authority for the purpose of the service of documents.

The central authority will serve the documents by post, or personally by hand if requested. Where personal service is specifically requested, the central authority can arrange for the document to be served by the police.

Most requests for service of process via a central authority will be accepted if the requirements set out below are met. There may be other requirements to meet in particular cases, and requesting authorities are therefore urged to provide detailed information including:

Requests for Service of Process
✓ EU Member States must explain why they are unable to serve the document directly;
✓ Details of any law/procedure in the requesting state which require the service of process to be via a central/judicial authority in the requested state;
✓ Specific instructions as to whether the documents **must** be served by hand. If no such instruction is provided the documents will be served by post;
✓ All dates of hearings or other deadlines should be stated clearly within the request;

PH-743

✓ The documents should be received by the central authority at least **six weeks** prior to court hearings or other deadlines involved;
✓ Details of any allowances and expenses to which a person asked to appear in proceedings abroad is entitled;
✓ The address of the court where the proceedings are to take place;
✓ The name and telephone number of an official of the overseas court from whom the person asked to appear can seek further information if necessary.

The person on whom a summons or judgment is served will be asked to sign a receipt and return it to the Home Office for transmission to the requesting authority, but the person is under no obligation to do so. The Home Office will advise the requesting authority whether the document has been delivered or whether it was not possible to serve the document.

In Scotland, the summons or judgment shall be served upon the person by either a police officer or police employee. The police officer or employee shall complete an execution of service which shall be returned to the requesting authority. The person shall be asked to sign a receipt, but is under no obligation to do so.

Back to Contents

Statements and Interviews

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Witness Statements	✓	✓

If the requesting authority's legal system does not require evidence to be taken on oath, the request should ask for the evidence to be obtained from a witness, suspect or victim as a statement. These interviews require the **consent** of the individual. Please see the website for a template request for witness evidence.

Requests for witness statements can be made on a law enforcement basis, rather than through MLA. The police or other law enforcement officers are not authorised to administer oaths in the UK. In the UK evidence can only be made subject to an oath before a court (see below). Unless a request specifically requires that evidence be given on oath, testimony will be taken without an oath being administered. This is considerably quicker and less resource intensive.

In cases where an individual refuses to co-operate with a statement or interview, it may be possible to compel the individual to attend court. However, the witness can exercise the right against self-incrimination and refuse to answer any questions at court.

Requests For Statements (Testimony) to be Taken by the Police
✓ Whether the individual to be interviewed is a witness, suspect or victim;
✓ Individual's address or, if not known, last known address;
✓ A list of questions to be asked should be provided;
✓ Language(s) which the person understands should be provided if possible;
✓ Details of any procedure to be followed in taking the evidence, including any rules on privilege which a witness or suspect may be entitled to claim. This will be complied with as far as is possible under UK law;
✓ Any caution or formal notification of rights which should be given to the witness under the law of the requesting state. This will be complied with as far as is possible under UK law.

Contacting Witnesses in the UK

Witnesses **must not** be contacted directly by letter, fax or telephone unless UK law enforcement agencies have first been informed, except where service of process can be served directly. Once UK law enforcement has been notified, the witness can be contacted directly.

Back to Contents

Evidence on Oath/in Court

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Witness Statements on Oath	X	✓

Requests for evidence can be 'sworn' or taken on oath by a court. It is also possible to take evidence in court without an oath (schedule 1, paragraph 3 of CICA provides that "*the court may take evidence on oath*") if this is allowed under the law of the requesting state.

Individuals can be compelled to attend court for the purposes of MLA requests under section 15 of CICA. However, schedule 1 of CICA makes it clear that a person cannot be compelled to give any evidence before a nominated court which he could not be compelled to give in criminal proceedings in the UK or if the criminal proceedings were being conducted in the requesting state. Of particular relevance in this context are:

- The privilege against self-incrimination; and
- The provisions in UK domestic law that a person *charged* with an offence cannot be compelled to give evidence in his own trial.

Requesting authorities must give careful consideration as to whether an individual should be compelled to attend court where they have already been uncooperative with the investigation/proceedings (for instance if they already refused to give a statement to the police). An individual can be compelled to attend court but may exercise the right against self-incrimination and remain silent so compelling a witness to court is unlikely to increase the chances of any evidence being obtained in some circumstances. Ultimately it is for the central authority to decide whether to nominate a court and the central authority will take into account all the circumstances when making this decision including details of any legal or procedural requirements under their domestic law and the effect on the investigation or prosecution if a person is not compelled to court.

In Scotland a Procurator Fiscal (Scottish Prosecutor) requires to crave a warrant from a Sheriff (lower judge) to cite the witness/suspect to the relevant Sheriff Court. The Sheriff is independent from the prosecution service and may refuse to grant the warrant if there is no dual criminality, insufficient facts provided in the letter of request or for any other reason he may see fit.

Request For Evidence (Testimony) To Be Taken Before A Court
✓ Expressly state whether the evidence must be taken before a court, and whether this must be on oath;
✓ Explain why it is necessary for the evidence to be taken in court, rather than by the police interview;
✓ Provide a list of questions to be asked;

✓ Provide details of the requesting authority's procedure to be followed in taking the evidence, including any rules on privilege which a witness or suspect may be entitled to claim. This will be complied with as far as is possible under UK law.
✓ Any caution or formal notification of rights which should be given to the witness or suspect under the law of the requesting state. Central authorities will aim to comply with such procedures and requirements as far as is possible under UK law.

Privilege

If an individual claims privilege under the law of the requesting state, and if the requesting authority concedes the claim, evidence will not be taken. Where the claim is not conceded, the evidence may be taken but will not be sent to the requesting authority until a court in the requesting state rules on the matter.

Back to Contents

COMMISSION OF INQUIRY INTO STATE CAPTURE

Hearings via Video or Telephone Conference

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Hearing by Video Conference	X	✓
Hearing by Telephone Conference	X	✓

Video Conference (Television Link)

The basis for hearing witnesses in the UK through video conferencing is section 30 of CICA. The video link must be made from UK court premises in the presence of a UK judge, in order to protect the rights of the witness. There is no legal framework for the use of commercial, private premises or Embassies.

If the requesting authority is unable to dial in to the UK, they will be charged for video conferencing by the Home Office. Scotland does not invoice requesting authorities for the costs of the television link.

Requests For Evidence Via Video Conference (Television Link)
✓ A minimum of **eight weeks'** notice given prior to the date of the video conferencing hearing;
✓ A proposed time of day that the link should be heard and the length of time that the witness is required;
✓ Email address of someone in the requesting authority that can be contacted at short notice who will provide technical assistance;
✓ Sufficient information to enable the central authority to identify and contact the witness(es);
✓ Details of the requirements of the procedure to be followed in taking the evidence, including any rules on privilege which a witness may be entitled to claim;
✓ Any caution or formal notification of rights which should be given to the witness under the law of the requesting state;
✓ Details (if known at the time) of the technical requirements for establishing the link to ensure compatibility.

Telephone Conference

The basis for hearing witnesses in the UK through telephone conferencing is section 31 and schedule 2 of CICA. This section only applies to relevant participating countries.

Requests For Evidence Via Telephone Conference
✓ A minimum of eight weeks' notice given prior to the date of the telephone link hearing;
✓ Confirmation that the witness has expressly agreed to give evidence via telephone link;
✓ The name and address of the witness to be questioned;
✓ Details of the procedure to be followed in taking the evidence, including any rules on privilege which a witness may be entitled to claim;
✓ Any caution or formal notification of rights which should be given to the witness or suspect under the law of the requesting state.

Back to Contents

COMMISSION OF INQUIRY INTO STATE CAPTURE

Asset Tracing

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Banking evidence	✓	X

All asset tracing should be completed on a police cooperation basis through financial intelligence units (FIUs).

There is **no central record of bank accounts held in the UK**. This information should be requested, where possible, on a police cooperation basis before making an MLA request.

See below for information on how to obtain banking evidence by production order, and requests for restraint and confiscation of assets.

Back to Contents

COMMISSION OF INQUIRY INTO STATE CAPTURE

Production Orders

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Production Order	X	✓

Production orders are used to obtain "special procedure material".

Examples of Special Procedure Material (non-exhaustive)
✓ Communications content; ✓ Banking evidence; ✓ Journalistic material; ✓ Records held by accountants etc.

In England & Wales and Northern Ireland, once a request for special procedure material is accepted by the central authority, the central authority will issue a direction under section 13 of CICA for the police to apply to the court for a production order under section 16 of CICA (production orders can also be obtained under Article 6 of the Proceeds of Crime Act 2002 (External Investigations) Order 2014 for the purposes of restraint and confiscation investigations). The application for a production order will be made in the Crown Court to a circuit judge and will normally be applied for on notice (*inter partes* to the organisation that holds the information) to ensure that the respondent (for example a bank) has an opportunity to be represented in the court that is hearing the application. Where the organisation does attend, the central authority will consult the requesting authority to ensure that the execution of the request will not breach any confidentiality requirement. A production order under the Proceeds of Crime Act 2002 (External Investigations) Order 2014 can be obtained *ex parte*.

In Scotland, a direction is sought from the Requested Advocate under section 13 of CICA to crave a search warrant under section 18 of CICA. The respondent will then submit the relevant documentation and witness statements to the police in answer to the warrant which in turn will be forwarded to the requesting authority.

Banking Evidence

Asset tracing should be completed before making a request for banking evidence (see above, regarding asset tracing).

Information to be Obtained *Before* Making a Request for Banking Evidence
✓ Name of the financial institution;
✓ Name of the account holder;
✓ Number of the account;

PH-751

✓ The address and/or number ("sort code") of the branch of the bank where the account is held

Once this information has been obtained the request should contain the following:

Request for Banking Evidence
✓ Details of account(s) (as above); and
✓ Grounds for believing that banks in the UK holds account(s) and to the extent available, which banks may be involved; and
✓ The time period over which the information is sought (an explanation must be given for any period that falls outside the time framework for the investigation); and
✓ Specific documents required (e.g. account opening information, bank statements, etc) and relevance to the investigation; and
✓ Confirmation that there is dual criminality.

Please be aware that the retention policies of banks vary at around **5 years**.

Please note that the Home Office receives a high volume of requests to obtain banking evidence in England & Wales and this may reduce the speed at which a request is executed.

Communications Content

Communications content can also be obtained via production order. Note it is possible to request the preservation of content via law enforcement cooperation pending the execution of an MLA request.

For communications data, see below.

Back to Contents

Search and Seizure

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Search & Seizure	X	✓

It is not sufficient for a request to be accompanied by a search warrant issued by an authority in the requesting state. Central and executing authorities in the UK do not have the authority to issue warrants themselves; they must be in a position to convince a court to issue a search warrant. In addition, requests for search and seizure require **dual criminality**. If the evidence requested can be obtained without obtaining a search warrant, the central authority will seek an alternative method of execution instead.

The following types of material cannot be the subject of a search warrant:

- "excluded material" which includes confidential journalistic records, medical records and samples, counselling records;
- "legally privileged" which includes material relating to advice provided by a solicitor to his client unless this material is held with the intention of furthering a criminal purpose;
- "special procedure material" which includes other confidential business records and non-confidential journalistic material (see production orders above).

Requests For Search and Seizure of Evidence
✓ Conditions in section 8 of Police and Criminal Evidence Act 1984 ('PACE') can be met;
✓ There is dual criminality;
✓ A full description of the criminal conduct concerned;
✓ The full address/addresses, or a precise description of any place to be searched;
✓ A full explanation as to where the specific material or type of material is expected to be recovered from, such as within the house, garage premises, garden premises;
✓ Details of how the place to be searched is connected with the case/suspected person;
✓ Full details of the specific material or type of material to be seized (it will not usually be sufficient to simply state "evidence relevant to the investigation") and; any information available which indicates that the material requested may be held on computer;
✓ Why the material requested is considered both relevant and important evidence to the investigation or proceedings;
✓ Why the evidence is thought to be on the particular premises or in the possession of the particular person concerned;
✓ Why the material would not be produced to a UK court if the natural or legal person

	holding the material were ordered to do so by means of a witnesses summons (this is to help ensure that applications to the UK courts for search warrants are successful and less likely to fail or be subject to subsequent legal challenge);
✓	Appropriate undertakings for the safekeeping and return of any seized evidence;
✓	If it is anticipated that law enforcement officers may come across 'special procedure material' during the course of a search;
✓	Details of any officials from the requesting state who wish to participate in the search and why their presence is necessary (note – we prefer officers from the requesting state to be involved in the search where possible);
✓	Any other information which would be of operational use to the executing authority in connection with the execution of the request.

Please note the search and seizure template form on the website. Please also refer to Section 4 on attendance of overseas law enforcement officers. It is also recommended that consideration of a search warrant is discussed on a law enforcement basis prior to the MLA request being made.

Seizure of Computers and other Storage Media

Under UK law, computers or images of them will not be provided direct to a requesting authority. This includes smartphones and other storage media; as such devices will always contain material which was not covered by the original warrant.

Upon seizure, these devices are examined by the UK police officers, who will ensure that the material was included in the original warrant and does not contain material which is legally privileged. Following a search of the material by UK police, it may be necessary for officers from the requesting state to visit the UK to be involved in examination.

Where further information is required about the offence or the material to be seized, depending on the particular circumstances, the Home Office will inform the requesting authorities without delay. Notification of interested parties is not required where an application is made for a search warrant.

Search and Seizure Requests in Scotland

The Crown Office in Scotland may direct a Procurator Fiscal (prosecutor) to obtain a search warrant from a Sheriff before the relevant Sheriff Court. With regard to the dual criminality test, the equivalent crime in Scotland must be an offence punishable by imprisonment (section 18(1)(b) of CICA). Neither the police nor HMRC can apply for a search warrant in Scotland. Interested parties are not notified of the application for a search warrant. The concept of legal privilege applies equally in Scotland.

Back to Contents

Communications Data

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Communications Data	✓	✓

Communications data refers to the "who", "when", "where" and "how" of a communication but not the **content** of the communication. This includes text messages and emails etc as well as phone calls. Communications data can be requested on a law enforcement cooperation basis.

If the request is accepted, the request will be referred to the relevant law enforcement agency, who will obtain the evidence under Chapter 2 of the Regulation of Investigatory Powers Act 2000 ('RIPA') as necessary.

If the requesting authority requires the evidence to be sworn in court by an employee of the communications company, the central authority will then nominate a court to receive the evidence under section 15 of CICA (see above for evidence on oath).

Communications companies in the UK normally retain IP data for between **30 days and 12 months**. Billing and communications data (cell site) is held for **6-12 months** for pay as you go phones and up to **six years** for contract phones. Specialised services such as cell dumps are normally only available for a matter of days. It is possible to request the preservation of communications data via law enforcement cooperation.

Requests for Communications Data
✓ Type of data required e.g. subscription details, incoming calls, outgoing calls;
✓ An explanation of the time periods of the data required;
✓ Why the information is necessary to the investigation. This must include the offence under investigation, how the specific person is linked to the investigation and how the data requested links to the offence and the person specified;
✓ Why the data is proportionate to the investigation e.g. what it is expected to show and how the data will be used;
✓ Information concerning the source of the telephone numbers;
✓ The exact date, time and place of the incident under investigation;
✓ Full details of the individuals involved in the incident and the roles they played;
✓ Why the objectives of the investigation cannot be achieved by other means;
✓ Explain whether the privacy of any individual not under investigation will be infringed, and why the circumstances of the case justify such an intrusion.

PH-755

Telephone and Address Information

If authorities require telephone numbers for businesses or people for non-evidential purposes it may be possible to locate information on 192.com or the BT Phonebook. This can provide information on a person or business phone number or address across different directories.

Back to Contents

COMMISSION OF INQUIRY INTO STATE CAPTURE

Live Interception of Communications

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Interception of Communications	X	✓

International requests for assistance in the interception of communications can **only** be made under Articles 17 to 22 of the MLAC. RIPA provides the UK legal framework governing the interception of the content of the communications in the course of its transmission. Interception can only be authorised for the purpose of preventing/detecting serious crime.

Serious Crime
✓ the offence or one of the offences is one in which a person who has attained the age of twenty-one (eighteen in England and Wales) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more; or
✓ the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

Before authorising a request restrictions may be imposed to prevent disclosure, in any proceedings outside of the UK, of intercept product which could not be adduced in the UK. The central authority must be satisfied that restrictions are in force which would prevent disclosure of, in any proceedings outside of the UK, intercept product which could not be adduced in the UK (i.e. it can only be used for intelligence purposes).

Requests For Interception
✓ The request is from a competent authority in a requesting state that has implemented the MLAC (EU Member States, Norway or Iceland);
✓ Confirmation that a lawful interception order or warrant has been issued in connection with a criminal investigation in the requesting state;
✓ An assurance that any intercept product will be handled in accordance with any restrictions imposed;
✓ Interception is necessary for the purpose of preventing or detecting serious crime;
✓ Why the objectives of the investigation cannot be achieved by other means;
✓ Interception must be proportionate to what is sought to be achieved; and
✓ Explain whether the privacy of any individual not under investigation will be infringed, and why the circumstances of the case justify such an intrusion.

Restraint (Freezing)

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Restraint of Assets	X	✓

Requests for Restraint of Assets *(not under EU mutual recognition instruments, see below)*

The purpose of a request for restraint is to preserve the value of assets located in the UK for confiscation. Before making a request to restrain assets located in the UK, the following should be completed so that the relevant information is included in the request for restraint:

***Before* Making a Request for Restraint of Assets**
1. Use law enforcement cooperation to identify and trace assets in the UK (see above); and,
2. Use, as necessary MLA, to obtain **evidence** of assets in the UK (e.g. to obtain banking evidence as referred to above).

Once this information has been obtained a request for restraint can be made to the court. Note that requests for restraint assets also require **dual criminality.** The following should be included in the request:

Request for Restraint of Assets
✓ There is dual criminality;
✓ Details of the ongoing (**not concluded**) criminal investigation into an acquisitive crime or money laundering or proceedings in the requesting state;
✓ The material facts of the case – including any defence or explanation put forward by the defendant/suspect, any facts that have come to light after the restraint order was made. This will enable the court to decide whether to maintain or discharge the restraint order;
✓ Why there is reasonable cause to believe that the defendant/accused named in the request has benefited (by obtaining money or other property) from his criminal conduct;
✓ Why there are reasonable grounds to believe that the property may be needed to satisfy an external order which has been or which may be made;
✓ Why the order is necessary – include an explanation that will enable the court to consider whether there is a real risk that the identified property will be dissipated if no order is made;
✓ The name, address, nationality, date and place of birth and present location of the

suspect(s) or defendants whose criminal conduct has given rise to anticipated confiscation or forfeiture proceedings;
✓ Details of the property to be restrained in the UK, the persons holding it and the link between the suspect and the property (this is important if the property to be restrained is held in the name of a third party such as a company or another person);
✓ Whether prior assistance in the case (including asset tracing assistance) has been provided and, if so, details of the UK authorities involved and details of the assistance already received. If assistance has not previously been sought or provided this should be clearly stated;
✓ Where applicable, details of any court orders already made in the requesting state against the suspect in respect of his or her property and a duly authenticated copy of that order certified by a person in his or her capacity as a judge, magistrate or officer of the relevant court of the requesting state, or by an official of the requesting authority. If no court orders have been made, this should be clearly stated;
✓ If possible, brief details of all known property held by the suspect outside the UK;
✓ State clearly that property in the UK must be restrained because there are insufficient property/assets elsewhere. If there are property/assets located elsewhere but these cannot be restrained, this must be clearly stated by the requesting authority;
✓ State clearly whether or not you object to the UK courts allowing the defendant access to restrained funds for use as living and legal expenses and **that you are content for the UK courts to assess what is a reasonable amount**.

Without this information a court will be unable to grant an order to effectively restrain assets or register an order to confiscate assets to allow it to be enforced. If the request is accepted, the central authority will decide who will execute a request and will refer it to the relevant executing authority (the CPS or the SFO) accordingly. The executing authority will consider the application before applying to the court to register the external order, in line with the Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 and section 447 of the Proceeds of Crime Act 2002.

The executing authority dealing with the request will make the appropriate applications to the Court for the assets to be restrained and will inform the requesting authority as soon as this has been done. A copy of the restraint order must be served upon the suspect and any other person known to be affected by it as soon as is practicable. The UK courts will require an acknowledgement that this has been completed otherwise the UK court may discharge the order. Note – a court may also discharge the order if proceedings are not started or the confiscation order is not registered within a reasonable time.

See the website for an example request in a restraint and confiscation case. Further guidance on restraint is available in the UK Guide to Asset Recovery.

There are also powers to assist to freeze property in relation to non-conviction based confiscation cases. Further details can be found in section 5.

Requests for Restraint of Instrumentalities of Crime

"Instrumentalities of crime" covers any property which has been, is or is intended to be used in connection with the commission of an offence. Section 4 of the Criminal Justice (International Co-operation) Act 1990 (Enforcement of Overseas Forfeiture Orders) Order 2005 ('2005 Forfeiture Order') enables a UK court to make a restraint order based on an overseas request.

Request for a Restraint of Instrumentalities of Crime
✓ Relevant instrumentalities in England and Wales have been identified; and
✓ A criminal investigation or proceedings for an offence have been started in the country from which the request was made; and
✓ Be for the purpose of facilitating the enforcement of any 'external forfeiture order' (made by a court in a designated country for the forfeiture and destruction, or the forfeiture and other disposal, of anything in respect of which a relevant offence has been committed or which was used or intended for use in connection with the commission of such an offence) which has yet to be made; and
✓ Provide reasonable grounds for believing that as a result of that investigation or those proceedings an external forfeiture order may be made against the person named in the request; and
✓ The material facts of the case – including any defence or explanation put forward by the defendant/suspect, any facts that have come to light after the restraint order was made. This enables the court to decide whether to maintain or discharge the order;
✓ Why the order is necessary – include an explanation that will enable the court to consider whether there is a real risk that the identified property will be dissipated if no order is made;
✓ The name, address, nationality, date and place of birth and present location of the suspect(s) or defendants whose criminal conduct has given rise to anticipated confiscation or forfeiture proceedings;
✓ Details of the property to be restrained in the UK, the persons holding it and the link between the suspect and the property (this is important if the property to be restrained is held in the name of a third party such as a company or another person);
✓ Whether prior assistance in the case (including asset tracing assistance) has been provided and, if so, details of the UK authorities involved and the assistance already received. If assistance has not previously been sought or provided this should be clearly stated;

PH-760

✓ Where applicable, details of any court orders already made in the requesting state against the suspect in respect of his or her property and a duly authenticated copy of that order certified by a person in his or her capacity as a judge, magistrate or officer of the relevant court of the requesting state, or by an official of the requesting authority. If no court orders have been made, this should be clearly stated;
✓ If possible, brief details of all known property held by the suspect outside the UK;
✓ State clearly that property in the UK must be restrained because there are insufficient property/assets elsewhere. If there are property/assets located elsewhere but these cannot be restrained, this must be clearly stated by the requesting authority;
✓ State clearly whether or not you object to the UK courts allowing the defendant access to restrained funds for use as living and legal expenses and that they are content for the UK courts to assess what is a reasonable amount.

Back to Contents

EU Freezing Order

A Freezing Order is an order for the protection of evidence or property, pending its transfer to a requesting state. Requests made under Council Framework Decision 2003/577/JHA are mutual recognition measures.

Part 2 of, and Schedules 1 and 2 to, the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 ("the Regulations") came into force on 3 December 2014. The Regulations transpose the Freezing Order measure in relation to property.

Freezing Orders for property must be sent by Member States to the relevant UK prosecuting authority for the purposes of recognition and execution (except terrorist property which must be sent to a central authority, see section 2).

Freezing Orders:
✓ From an EU Member State;
✓ The order must relate to criminal proceedings instituted in the Member State, or to a criminal investigation being carried out there;
✓ The order must prohibit dealing with property which is in the UK, and which the appropriate overseas court or authority considers to be property that has been or is likely to be used for the purposes of criminal conduct, or is the proceeds of criminal conduct (both tainted and untainted assets);
✓ The criminal conduct must not be an act of terrorism, or for the purpose of committing terrorism;
✓ Accompanied by a certificate which is: a) signed by (including electronically) or on behalf of the court or authority which made or confirmed the order, (b) include a statement as to the accuracy of the information given in it (c) translated into English;
✓ The order must be accompanied by another court order from the requesting state, for the confiscation of the property, or, if this is not available, the certificate must indicate when such an order is likely to be sent.
✓ State clearly whether the case is a fraud and/ bribery and corruption case, whether it is of a serious and complex nature, and whether the activity is capable of affecting the reputation of the requesting state as a safe place to do business (this will aid the UK's administration of these cases, by ensuring that they are dealt with by the appropriate authority).

Back to Contents

Confiscation & Forfeiture

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Confiscation of Assets	X	✓

Requests for Confiscation *(not under EU mutual recognition instruments, see below)*

Confiscation is the registering and enforcing of the requesting state's order against assets in the UK. Requests for confiscation of assets require **dual criminality**.

Request for Confiscation of Property
✓ There is dual criminality;
✓ Person named in the order is convicted and no appeal is outstanding in respect of that conviction;
✓ The order is in force and is not subject to appeal;
✓ All or a certain amount of the sum payable under the order remains unpaid in the territory of the requesting state or that other property recoverable under the order remains un-recovered there;
✓ The order has the purpose of recovering property, or the value of property received in connection with the commission of crime;
✓ The order made can be enforced outside the jurisdiction of the requesting state.
✓ The original or duly authenticated copy of the order must be provided with the request;
✓ The material facts of the case – including any defence or explanation put forward by the defendant/suspect, any facts that have come to light after the restraint order was made. This will enable the court to decide whether to maintain or discharge the restraint order;
✓ Why the order is necessary – include an explanation that will enable the court to consider whether there is a real risk that the identified property will be dissipated if no order is made;
✓ The name, address, nationality, date and place of birth and present location of the suspect(s) or defendants whose criminal conduct has given rise to anticipated confiscation or forfeiture proceedings;
✓ Details of the property to be confiscated in the UK, the persons holding it and the link between the suspect and the property (this is important if the property to be restrained is held in the name of a third party such as a company or another person);

PH-763

✓ Whether prior assistance in the case (including asset tracing assistance) has been provided and, if so, details of the UK authorities involved and details of the assistance already received. If assistance has not previously been sought or provided this should be clearly stated;
✓ Where applicable, details of any court orders already made in the requesting state against the suspect in respect of his or her property and a duly authenticated copy of that order certified by a person in his or her capacity as a judge, magistrate or officer of the relevant court of the requesting state, or by an official of the requesting authority. If no court orders have been made, this should be clearly stated;
✓ If possible, brief details of all known property held by the suspect outside the UK.

If the request is accepted, the central authority will decide who will execute a request and will refer it to the relevant authority accordingly, in line with the Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005. Once referred, and provided that all the conditions are satisfied, the executing authority can ask the court to register the external order. This enables the payment to be enforced.

See the website for an example request in a restraint and confiscation case. Further guidance on restraint is available in the UK Guide to Asset Recovery.

Asset Disposal

Once the assets have been realised they will be disposed of under one of three processes:

- Stolen State asset cases that fall under the provisions of the United Nations Convention Against Corruption (UNCAC) will be returned to the recipient country less reasonable expenses;
- Cases that do not fall under the provisions of UNCAC can be shared with the recipient country if it enters into an asset sharing agreement with the UK. The UK seeks to establish asset sharing agreements wherever possible (under Article 16 of Council Framework Decision 2006/783/JHA there is an asset share of 50:50 in cases involving 10,000 Euros and above);
- If there is no formal agreement with a country or territory, there are administrative arrangements that allow assets to be shared on a case-by-case basis.

In the absence of any asset sharing agreement the assets will be retained by the UK and disposed of according to domestic law.

Forfeiture of Instrumentalities of Crime

Forfeiture orders allow for the deprivation or disposal of property which has been used, or which is intended to be used, in the commission of a criminal offence. The 2005 Forfeiture Order allows for a forfeiture order which has been made overseas to be enforced in the UK. The 2005

Order applies to any offence that corresponds to or which is similar to, an offence under the law of England and Wales. Different Orders apply to Scotland and Northern Ireland.

Request for Forfeiture of the Instrumentalities of Crime
✓ Person named in the order is convicted and no appeal is outstanding in respect of that conviction; and
✓ The order is in force and is not subject to appeal.
✓ The original or duly authenticated copy of the order must be provided with the request;
✓ The material facts of the case – including any defence or explanation put forward by the defendant/suspect, any facts that have come to light after the restraint order was made. This will enable the court to decide whether to maintain or discharge the restraint order;
✓ Why the order is necessary – include an explanation that will enable the court to consider whether there is a real risk that the identified property will be dissipated if no order is made;
✓ The name, address, nationality, date and place of birth and present location of the suspect(s) or defendants whose criminal conduct has given rise to anticipated confiscation or forfeiture proceedings;
✓ Details of the property to be forfeited in the UK, the persons holding it and the link between the suspect and the property (this is important if the property to be restrained is held in the name of a third party such as a company or another person);
✓ Whether prior assistance in the case (including asset tracing assistance) has been provided and, if so, details of the UK authorities involved and details of the assistance already received. If assistance has not previously been sought or provided this should be clearly stated;
✓ Where applicable, details of any court orders already made in the requesting state against the suspect in respect of his or her property and a duly authenticated copy- of that order certified by a person in his or her capacity as a judge, magistrate or officer of the relevant court of the requesting state, or by an official of the requesting authority. If no court orders have been made, this should be clearly stated;
✓ If possible, brief details of all known property held by the suspect outside the UK;
✓ State clearly that property in the UK must be forfeited because there are insufficient property/assets elsewhere. If there are property/assets located elsewhere but these cannot be restrained, this must be clearly stated by the requesting authority.

PH-765

EU Confiscation Order

Part 2 of, and Schedules 1 and 2 to, the Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014 ("the Regulations") came into force on 3 December 2014. These transpose the Confiscation Order measure.

Confiscation Orders must be sent by Member States to the relevant UK prosecuting authority for the purposes of recognition and execution (see section 2).

Confiscation Order
✓ Must be from an EU Member State;
✓ The property must have been used for the purposes of criminal conduct, or must be the proceeds of criminal conduct (both tainted and untainted assets);
✓ A person must have been **convicted** of that criminal conduct in the requesting state;
✓ The confiscation order must have been made at the **conclusion** of the proceedings that gave rise to the conviction;
✓ Must be accompanied by a certificate which is a) signed by (including electronically) or on behalf of the court or authority which made or confirmed the order, (b) include a statement as to the accuracy of the information given in it (c) translated into English;
✓ State clearly whether the case is a fraud and/ bribery and corruption case, whether it is of a serious and complex nature, and whether the activity is capable of affecting the reputation of the requesting state as a safe place to do business (this will aid the UK's administration of these cases, by ensuring that they are dealt with by the appropriate authority).

Back to Contents

Temporary Transfer of a Prisoner for Purposes of Investigation

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Temporary Prisoner Transfer	X	✓

Under section 5 of the Criminal Justice (International Cooperation) Act 1990, a UK prisoner can be *temporarily* transferred abroad to assist with overseas criminal investigations and proceedings. Prisoners cannot be transferred from the UK without their consent. Requests for temporary transfer of prisoners must be sent to a central authority.

Before agreeing to the transfer the relevant central authority must be satisfied that the presence of the prisoner is not already required in that part of the UK for the purposes of investigations or proceedings and that the transfer would not prolong the prisoner's period of detention.

Where the transfer is agreed with the requesting authority, the central authority arranges for:

- the prisoner in custody to be taken to a departure point in the UK and to be delivered into the custody of a person representing the requesting authority;
- for the prisoner to be escorted back to the UK by the requesting authority;
- the subsequent transfer of the prisoner in custody from the arrival point in the UK to his or her place of detention.

The costs of escorting and accommodating prisoners from their point of departure from the UK to their point of return to the UK are met by the requesting authority.

The central authority will liaise with the respective prison services in England and Wales, Scotland and Northern Ireland to ensure that the prisoner is taken to a point of departure in the UK and then taken back into prison custody when the requesting authority has completed their process.

England & Wales

National Offender Management Services ('NOMS') would expect a **minimum of three weeks'** notice to arrange the transfer of a prisoner from an English prison to a point of departure. This is because transfer between prisons takes place by scheduled booked transport and advance notice is required. The contact details for the relevant part of NOMS who can deal with these requests can be found below.

Northern Ireland

Where a request has been made for a transfer of a prisoner from Northern Irish custody the prison service in this jurisdiction will manage the handover of prisoners in line with their operational instructions. For further information contact the Northern Ireland Prison Service.

Scotland

Where a request is to be made for the transfer of a prisoner in a Scottish prison, the request must be sent to the Scottish Central authority which will liaise with the Scottish Prison Service. When it is agreed the request will be executed the Scottish Prison Service would also expect a minimum of three weeks notice for the same reasons as set out above.

However, given the cost, staff resources and risk assessment in ensuring safety to the public in transferring a prisoner across borders, consideration should be given to the prisoner giving evidence by video conference or, as has happened in Scotland, the prisoner giving evidence before a Scottish Court constituted with the prosecution, defence and judge of the requesting jurisdiction.

For further information contact the International Cooperation Unit at the Crown Office or for practical arrangements on the return of the prisoner, the Scottish Prison Service.

Temporary Transfer of Prisoners to the Requesting State to Assist an Investigation
✓ Dates on which the presence abroad of the prisoner is required, including the dates on which the court or other proceedings for which the prisoner is required will commence and are likely to be concluded;
✓ Information for the purpose of obtaining the prisoner's consent to the transfer and satisfying the UK authorities that arrangements will be made to keep the prisoner in secure custody such as: • whether the prisoner will have immunity from prosecution for previous offences; • details of proposed arrangements for collecting the prisoner from and returning the prisoner to the UK; • details of the type of secure accommodation in which the prisoner will be held in the requesting state; • details of the escort available abroad to and from the secure accommodation.

Transfer of a Prisoner for the Purpose of Serving the Remainder of a Prison Sentence *(non-MLA Prisoner Transfer)*

The MLA central authorities do not deal with requests for the transfer of prisoners for purposes of ensuring they serve the remainder of a prison sentence *or any* other non-MLA basis. The authority for these requests is (and general queries on all types of prisoner transfer):

PH-768

England & Wales Contact Details for Prisoner Transfer Requests	
Cross Border Transfers Section Offender Safety, Rights and Responsibilities Group Post Point 4.10 4th Floor, Clive House 70 Petty France London SW1H 9EX	Tel: +44 300 0 475691 Fax: +44 300 0 476857 Email: ERDForeignNationals@noms.gsi.gov.uk

Northern Ireland Contact Details for Prisoner Transfer Requests	
Establishment Support Branch Room 211, Dundonald House Upper Newtownards Road Belfast BT4 3SU	Tel: +44 2890 525310 Fax: +44 2890 525315

Scotland Contact Details for Prisoner Transfer Requests	
International Cooperation Unit Crown Office and Procurator Fiscal Service 25 Chambers Street Edinburgh EH1 1LA	Tel: +44 131 243 8152 Fax: +44 131 243 8153
The Scottish Prison Service Legal Services Branch Calton House 5 Redheughs Rigg Edinburgh EH12 9HW	Tel: +44 1312448745

Back to Contents

PH-769

Passport Information and Immigration Status

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Passport Records/Immigration Status	✓	✓

Requests for this information can be sought through law enforcement cooperation. All requests will be referred to HM Passport Office or UK Visas and Immigration.

Passport Information / Immigration Status
✓ Details of person (name, date of birth and place of birth if known);
✓ Passport number (current and previous);
✓ State whether the request relates to the prevention and detection of crime or apprehension of prosecution of an offender;
✓ How the data being sought links to the offence being investigated.

Back to Contents

Transfer of Proceedings

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Transfer of Proceedings	X	✓

Proceedings should take place in the jurisdiction where the majority of the criminality occurred, or, if this is not possible, where the harm was felt. In practice, the UK's common law system of adversarial proceedings and live witness examination tends to be incompatible with a process in which the proceedings had been transferred from another jurisdiction.

The UK is not a signatory to the Council of Europe Convention on the Transfer of Proceedings in Criminal Matters 1972 and has a reservation to the Council of Europe Convention on Mutual Assistance in Criminal Matters 1959 which states that "*…the Government of the United Kingdom reserves the right not to apply Article 21".*

However, incoming requests to transfer proceedings to or from the UK are decided on a case by case basis according to the criteria set out below.

Note: A UK bank account is not a sufficient link to transfer proceedings to the UK.

Request for Transfer of Proceedings
✓ The offence leading to the criminal proceedings must constitute a crime in both the UK and the requesting state;
✓ There must be evidence of a clear and established link to the UK;
✓ The request must be made as soon as is reasonably possible. Any unreasonable delay (more than 5 years) must be explained;
✓ The request is not *de minimis* (see above);
✓ Must be translated into English (including supporting documents).

If accepted, the request will be forwarded to the relevant police force, and the case will be given the same status and priority as would be given to a similar domestic case. In England, Wales and Northern Ireland it is up to the police to decide whether an investigation is conducted. In Scotland the Crown Office will instruct the police to commence an investigation and shall consider the results before any decision on prosecution is made.

Article 17 of the Directive Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime

Article 17 of this directive deals with victims of crime in an EU Member State other than where they reside, who wish to make a complaint in their Member State of residence if they are unable to do so where the offence was committed or, in the event of a serious offence, they do not wish to do so. The following criteria are applied to requests to transfer proceedings to the UK under this provision:

Request for Transfer of Proceedings under Article 17
✓ Explain why the Member State in which the complaint was made does not have competency to investigate the complaint; and
✓ Explain why the victim was unable to make such a complaint in the state where the offence was committed; *or* in the case of a serious offence, the victim did not wish to do so.
✓ An English translation should be provided

If accepted, the request will be forwarded to the relevant police force to consider opening an investigation, and the case will be given the same status and priority as would be given to a similar domestic case.

Spontaneous Exchange of Information

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Spontaneous Exchange	✓	✓

If a central authority has information relating to a criminal offence which may lead or relate to an MLA request by a country, the UK may exchange this information with a country without the need for a request. This is possible under Article 7 of the MLAC 2000 and under bilateral MLA treaties. Spontaneous exchange of information is also possible via police cooperation routes and will be channelled through the NCA.

Back to Contents

PH-772

Criminal Records

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Criminal Records	✓	✓

Although requests for criminal records may form part of a wider formal MLA request, requesting authorities **should not** obtain criminal record information from the Home Office (England, Wales and Northern Ireland) or the Crown Office (Scotland).

EU Member States

The bases for exchanging criminal records between EU Member States are Framework Decision 2009/315/JHA, on the organisation and content of the exchange of information extracted from the criminal record between Member States together with Council Decision 2009/316/JHA on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA. These are collectively known as ECRIS (European Criminal Record Information System).

EU Member States must make requests for criminal records via their own central authority for the exchange of criminal records. The criminal record information provided through ECRIS is transmitted through a standardised format which facilitates automatic translation and recognition of criminal offences.

If a central authority (Home Office or Crown Office) receives a request for criminal records from an EU Member State the request will be redirected to the UK Central Authority for the Exchange of Criminal Records. For more background information please visit the HOME OFFICE-ECR website.

Requests from Non-EU Member States

Requests for criminal records from countries outside of the EU should be made on a law enforcement cooperation basis via the NCA.

Back to Contents

PH-773

Judicial Records

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Judicial Records	✓	✓

In England & Wales and Northern Ireland, all criminal cases start in the Magistrates Court. More serious cases are then transferred to the Crown Court. The name of the court of conviction and date of sentence can be found on the criminal record (see above).

In Scotland, the prosecutor can raise proceedings in the Justice of the Peace Court or Sheriff Court. Cases related to serious crime begin in the Sheriff court and can then continue to proceed there or be transferred to the High Court of Justiciary.

Court Certificates

EU Member States should request court certificates **directly from the relevant court**. A copy of the criminal record (see above) must be attached to the request, which will also contain the name of the sentencing court. Contact details for courts in England & Wales, Northern Ireland, or Scotland can be found on their respective websites.

Requests from EU Member States sent to the Home Office or Crown Office in error, will be referred to the relevant court (if the name of the court has been provided by the requesting state), but this may delay a substantive response.

Non- EU Member States must request court certificates from the relevant central authority (Home Office or Crown Office).

A Court Certificate from a Magistrates Court (Memorandum of Conviction) may Contain:
✓ Defendant's personal details;
✓ Whether or not the defendant was represented;
✓ Type of offence;
✓ Plea;
✓ Type of sanction (including length of sentence imposed).

A Court Certificate from a Crown Court (Certificate of Conviction) may Contain:
✓ Defendant's personal details;

✓ Details of the legal representatives for the defence and prosecution;
✓ Whether the defendant was in detention during the trial;
✓ Date of hearing;
✓ Date of conviction;
✓ Date of sentence;
✓ Charges against the defendant, plea and verdict.

If *specifically* Requested the Court may also Provide
✓ Information on the use of an interpreter during the proceedings, and if not used, the reasons why;
✓ The identity of defence counsel in the proceedings;
✓ The status of any appeal against Conviction(s)/ Sentence(s).

Trial Transcripts / Sentencing Remarks

A Magistrates Court is not a court of record and there will be no court transcript.

In England, Wales and Northern Ireland, more serious criminal cases are dealt with by a Crown Court and a full court transcript of the trial may be available. However, there is no written note made and the comments are recorded on a tape which is kept for a certain number of years. Transcripts obtained in this way can be very expensive, as the transcription service is provided by a private company who charge by the folio (72 words). This is regardless of whether the request is from a UK authority or from an overseas authority.

In Scotland, a transcript of proceedings is only retained in cases of serious crime where the accused is indicted before a Judge / Sheriff and a jury. However, the transcript is the property of the court and an application must be made to the Court for that to be disclosed. The cost of any transcript will be high and will require to be met by the requesting judicial authority.

Rather than obtain the whole trial transcript, it is possible to obtain a smaller part of the transcript known as the 'sentencing remarks'. This is the final part of the trial where the judge at the Crown Court makes a summary of the case when sentencing the defendant. However, this is not the same as the formal written summary used in other jurisdictions and the level of detail the judge will provide (e.g. about the circumstances of the offence and the conduct of the defendant) will vary from case to case.

PH-775

To obtain a transcript or sentencing remarks a request can be made to the Home Office or Crown Office for a transcript of the tapes, but please be aware that transcripts are not retained indefinitely. However, in most cases the costs of obtaining the transcripts or sentencing remarks must be met by the requesting authority, as they are considered costs of an extraordinary nature. Further details on the provision of transcripts, including prices, can be found on the form EX107 on the Ministry of Justice website.

Request for Transcripts or Sentencing Remarks
✓ A copy of the ECRIS report if the request is from an EU Member State, or if the request is from a non-EU member state, the following information must be included: • Name of relevant court • Date of hearing • Date of sentence
✓ Written confirmation in English that such evidence is required;
✓ Written confirmation in English that the requesting authority will pay for the costs of acquiring such evidence.

If these confirmations are not received at the time of the request a substantive response is likely to be delayed.

Back to Contents

Other Requests for MLA

Intimate/Non-Intimate Samples (including DNA)

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Intimate/Non-Intimate Samples	✓	✓

The UK can consider an MLA request for intimate samples to be taken from an individual; however the UK has no power to compel an individual to do so.

A DNA profile which is held by the UK will generally not be transferred abroad as part of an MLA request for the purposes of matching it to a crime scene profile. If a request for DNA matching is made, the requesting authority should send the crime scene profile to the UK for matching. This enables it to be checked against the individual concerned and against other profiles held on the UK's National DNA database. This can be made on a law enforcement cooperation basis.

EU Freezing Order for Evidence

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
EU Freezing Order	X	✓

Sections 20-25 of CICA implemented the in relation to evidence. Freezing orders in relation to evidence must be sent to the Home Office (see section 2).

Freezing Order (evidence)
✓ The request must be from an EU Member State;
✓ The request must be to freeze evidence (not property/money);
✓ The request must be in relation to a listed offence category;
✓ The request must be accompanied by a certificate which is a) signed by (including electronically) or on behalf of the court or authority which made or confirmed the order, (b) include a statement as to the accuracy of the information given in it (c) translated into English (or, if appropriate, Welsh);

Under section 24 of CICA, once evidence has been frozen, it must be retained until instructions have been given to transfer the evidence to the requesting state, or to release it.

PH-777

Account Monitoring Orders

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Account Monitoring Order	X	✓

An Account Monitoring Order enables transactions on a particular account to be monitored for a specified period of time. Account Monitoring Orders under section 35 of CICA **only** apply to an investigation into serious criminal conduct by a 'participating country'.

Requests For An Account Monitoring Order under CICA:
✓ The request must be from a participating country (EU Member States, Iceland, Japan, Norway, Switzerland and the USA);
✓ Specify a 'financial institution' and accounts held there by a specified person;
✓ There is an investigation in the requesting state into criminal conduct;
✓ The order is sought for the purposes of the investigation.

Account Monitoring Orders can also be requested under Part 5 of the Proceeds of Crime (External Investigations) Order 2014 (POCA Order).

Requests For An Account Monitoring Order under Part 5 of the POCA Order:
✓ Account Monitoring Orders may be obtained for the purpose of an external investigation, relating to a criminal investigation or criminal proceedings in the requesting state provided that the investigation falls within the definition set out in Part 8 of POCA 2002:
✓ Part 8 of POCA deals with two types of investigation. ✓ A confiscation investigation, which is an investigation into: a) whether a person has benefited from his criminal conduct, or: b) the extent or whereabouts of his benefit from his criminal conduct. ✓ A civil recovery investigation, which is an investigation into: a) whether property is recoverable property or associated property b) who holds the property, or c) its extent or whereabouts.
✓ The request must show that there are reasonable grounds for believing that the account information requested is of substantial value to the external investigation, and that it is in the public interest for the account information to be provided;

Company Records

Type of Assistance	Law Enforcement Cooperation	Judicial Cooperation
Company Records	✓	✓

Information about a company in England, Wales, Northern Ireland or Scotland, that is **not** required as evidence can be found on the Companies House website. This website has a search engine called WebCHeck. Companies House also offer other services to help find information on companies, some of which is free.

Joint Investigation Teams

A Joint Investigation Team ('JIT') is an investigation team set up for a set period, based on an agreement between two or more States and/or competent authorities, for a specific purpose. A JIT allows team members from different countries to share information without the need for a formal letter of request, and is therefore an *alternative* to MLA.

A JIT can be considered in cases where close and co-ordinated co-operation between countries is required to effectively and efficiently investigate crime. A JIT can be set up under:

- Council Framework Decision on Joint Investigation Teams (2002/465/JHA);
- Convention on Mutual Assistance in Criminal Matters between the Member States;
- Second Additional Protocol to the Council of Europe Convention on Mutual Assistance;
- Convention on Mutual Assistance and Cooperation between Customs Administrations;
- A specific bilateral/multilateral agreement with the participants in the JIT.

Eurojust has developed an expertise in drafting and negotiating JITs and is also a potential source of funding for JITs. Prosecutors or courts contemplating a JIT with the UK are advised to consult their National Desk at Eurojust to discuss the case further.

Back to Contents

PH-779

SECTION 4: Foreign Officers in the UK

If officers from the requesting state wish to be present during the execution of an MLA request, for example to participate in a search or to be present during the interview of a witness, this must also be requested in the request. The central authority, in conjunction with the authority executing the request in the UK, will determine whether this is appropriate.

The requesting authority must give reasons as to why officers from the requesting state should be present. For example, if it is a very complex case, or is a request for search and seizure, it may be beneficial to have the investigating officer present. However, if it is not justified for a foreign officer of the requesting state to be present this request will be refused.

Even if the presence of foreign officers is accepted and the request is successfully executed, evidence will not automatically be given to the officers who were present during the execution. However, it may on occasion be practical to transfer the evidence through accompanying officers. In this case UK police must seek authorisation from the central authority.

Notifying the UK of Law Enforcement Officers Travelling to the UK

The relevant local police force in the UK **must** be made aware in advance if officers for the requesting state are due to travel to the UK. However, if the requesting state is unable to contact / identify the local police force, the NCA can assist and pass on notification.

The relevant local police force in the UK **must** also be notified in advance if foreign law enforcement officers are due to travel to the UK to conduct official **business even if this is not pursuant to MLA**.

Back to Contents

PH-780

SECTION 5: Civil Matters

MLA requests to the UK relating to civil matters are dealt with by different authorities than those dealing with MLA requests in criminal matters.

Under the Civil Procedure Rules Part 34, MLA requests to and from the UK relating to civil matters are dealt with separately from criminal requests. Obtaining evidence from other jurisdictions in respect to civil litigation (which encompasses commercial litigation) is included within the Evidence (Proceedings in Other Jurisdictions) Act 1975.

Requests for the Service Of Documents in International Civil Cases in England & Wales and Northern Ireland	
Premium Service Legalisation Office Foreign & Commonwealth Office Old Admiralty Building London SW1A 2PA	Tel: +44 207 008 4126 Email: SOPEnquiries@fco.gov.uk

Request for Taking Evidence in Civil Matters in England & Wales and Northern Ireland
Foreign Process Section Room E16 Royal Courts of Justice Strand London WC2A 2LL

Request For Assistance for all Civil Matters in Scotland
The Central Authority & International Law Team Scottish Government Justice Directorate St Andrew's House Regent Road Edinburgh EH1 3DG

PH-781

Civil Forfeiture of Assets

Requests for a civil forfeiture of assets should be sent to a specialist team in the Home Office:

Request for Civil Forfeiture	
Strategic Centre for Organised Crime - Pursue Office for Security and Counter-Terrorism Home Office 6th Floor Peel Building 2 Marsham Street London SW1P 4DF	Tel: +44 20 7035 1567

European Judicial Network in Civil and Commercial Matters

There is a European Judicial Network (EJN) for Civil and Commercial Matters website where a large quantity of information about the Member States, Community law, European law and various aspects of civil and commercial law can be found.

Back to Contents

the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

International Legal Obligations

Extradition and Mutual Legal Assistance in criminal matters treaties

1. South Africa currently has extradition agreements with the following countries:

- **Algeria**
  - Approval to ratify on 11 November 2002
  - Not yet in force
- **Argentina** (GG 40978, GeN 519, 14 Jul 2017)
- **Australia**
  - Approval to ratify by Parliament on 9 November 2000
  - Notice in Government Gazette 7132 of 1 August 2001
- **Botswana**
- **Canada**
  - Approval to ratify by Parliament on 3 April 2001
  - Notice in Government Gazette 7063 of 18 May 2001
- **China**:
  - Approval to ratify on 11 November 2002
  - Instruments of ratification exchanged on 18 October 2004
  - Entered into force on 17 November 2004
- **Egypt**:
  - Approval to ratify on 11 November 2002
  - Instruments of ratification exchanged on 16 September 2003
  - Entered into force on 16 September 2003
  - Notice in Government Gazette 26497 of 2 July 2004
- **India**
  - Approval to ratify on 9 November 2004
  - Instruments of ratification exchanged on 6 December 2005
  - Entered into force on 16 December 2005
- **Israel**
- **Lesotho**
  - Approval to ratify by Parliament on 7 November 2001
  - Entered into force on 23 December 2003
  - Notice published in Government Gazette 26375 of 28 May 2004
- **Malawi**
- **Nigeria**
  - Approval to ratify on 11 November 2002
  - Not yet in force

7.4k
Shares

PH-783

- **United States of America**
  - Instruments of Ratification exchanged on 25 June 2001
  - Approval to ratify on 9 November 2000
  - Notice in Government Gazette 7100 of 29 June 2001

2. Treaties negotiated but not yet signed

- **Brazil** (MLA)
- **Cuba** (Extradition and MLA)
- **Hungary** (Extradition) (Covered under COE Convention on Extradition)
- **Namibia** (Extradition and MLA)
- **Republic of Korea** (Extradition and MLA)
- **Taiwan** (MLA arrangement)
- **United States of Mexico** (Extradition and MLA)
- **United Arab Emirates** (Extradition) MLA to be finalised during second round of negotiations
- **Zambia** (Extradition and MLA)

3. Extradition and Mutual Legal Assistance Treaties signed but not yet ratified:

- **Hong Kong** (Extradition and MLA)
  - Signed on 20 February 2009
  - To be submitted to Parliament for ratification
- **Iran**
  - Signed on 31 August 2004
  - Submitted to Parliament for ratification

4. **The Treaty with the Republic of China (Taiwan),** signed on 30 December 1987, is deemed to be terminated in terms of the Memorandum of Understanding between the Government of the Republic of South Africa (RSA) and the Government of the People's Republic of China (PRC) on the Establishment of diplomatic relations between the RSA and the PRC.

5. South Africa has Mutual Legal Assistance in Criminal Matters Treaties with the following countries:

- **Algeria**
  - Ratified by Parliament on 11 November 2002
  - Not yet in force
- **Argentina** (Extradition and MLA) GG 40978, GeN 518, 14 Jul 2017
  - Ratified by Parliament on 29 August 2007
  - Entered into force 16 October 2015
- **Canada**
  - Ratified by Parliament on 3 April 2001
  - Entered into force 5 May 2001
- **China**
  - Ratified by Parliament on 21 October 2003
  - Instruments of ratification exchanged on 18 October 2004
  - Entered into force on 17 November 2004
- **Egypt**
  - Ratified by Parliament on 11 November 2002
  - Entered into force on 16 September 2003
- **France**
  - Ratified by Parliament on 11 November 2002
  - Entered into force on 1 March 2004
  - Notice in Government Gazette 27371 of 18 March 2005

7.4k
Shares

PH-784

- Approval to ratify on 3 November 2004
- Instruments of ratification exchanged on 6 December 2005
- Entered into force on 6 December 2005

- **Lesotho**
  - Ratified by Parliament on 7 November 2001
  - Entered into force on 23 December 2003

- **Nigeria**
  - Ratified by Parliament on 11 November 2002
  - Not yet in force

- **USA**
  - Ratified by Parliament on 9 November 2000
  - Entered into force on 25 June 2001

6. The Department is currently busy setting up **negotiations for the conclusion of extradition and mutual legal assistance treaties with various countries including**:

- **Brazil**
- **Chile**
- **Ethiopia**
- **Pakistan**
- **Paraguay**
- **Peru**
- **Tunisia**
- **Uruguay**
- **Venezuela**

7. South Africa has also designated **Ireland, Zimbabwe, Namibia** and the **United Kingdom** in terms of section 3(2) of the Extradition Act.

8. South Africa's accession to the Council of Europe's Convention on Extradition entered into force on 13 May 2003. A request was also directed to the Council of Europe that South Africa accede to the Convention on Mutual Legal Assistance. The Council of Ministers approved that South Africa accede to the MLA Convention. South Africa must now indicate any possible reservations.

9. In terms of the Extradition Act, any arrangement made with any foreign State which, by virtue of the provisions of the Extradition Acts, 1870 to 1906 of the Parliament of the United Kingdom as applied in the Republic, was in force in respect of the Republic immediately prior to the date of commencement of the Act shall be deemed to be an agreement entered into and published on the said date by the President under the Act.

10. SADC Protocols on Extradition and Mutual Legal Assistance (MLA) in Criminal Matters

- This Protocol was signed by Summit on 3 October 2002 and ratified by Parliament on 14 April 2003. The Protocol on Extradition entered into force on 18 August 2006. The MLA Protocol still needs one ratification before it can enter into force (to be confirmed by SADC Secretariat).

11. African Union Convention on Extradition

- The African Convention on Extradition was finalized during a meeting of legal experts held in Ethiopia from 4 – 8 April 2001. The Department of Foreign Affairs was requested to determine the delay in this matter.

Copyright © 2019 The Department of Justice and Constitutional Development

7.4k
Shares

PH-785

The US and South Africa are stronger together

I will especially strive to help more women to achieve their professional goals, writes new US ambassador to SA **Lana Marks**.

Time up for the Guptas? Parliament approves extradition treaty with UAE

2018-11-15 17:19

Daniel Bugan, Correspondent

news24

The National Assembly has approved the signing and ratification of an extradition treaty with the United Arab Emirates (UAE), which could see the Gupta brothers brought to book for state capture allegations.

The adoption of the extradition and mutual legal assistance treaties on criminal matters was unanimously approved by all political parties on Thursday.

The step is a culmination of an eight-year process which began with discussions between the two countries in February 2010.

ACDP MP Steve Swart welcomed the ratifying of the agreements, which he said would pave the way for the Guptas to return to South Africa.

However, he questioned why the process took so long to come to fruition.

"I raised my concerns regarding the Guptas in April 2016, and only now, two and a half years later, are we seeing the agreements being ratified."

ANC MP Gijimani Skosana deflected Swart's criticism.

"It takes time for bilateral agreements to reach consensus. It took us eight years to get to the point of having the treaty approved," said Solana.

He said the treaty reaffirmed the ANC's commitment to act against international terrorism and crime.

DA MP Glynis Breytenbach said the DA welcomed the adoption of the treaty and hoped that the Guptas would be held to account for "looting our fiscus and that there will be less place for them to hide".

Justice Minister Michael Masutha signed both treaties on September 25 in Abu Dhabi after getting authorisation from President Cyril Ramaphosa to do so on behalf of the South African government.

The UAE is made up of Abu Dhabi, Ajman, the popular Dubai, Fujairah, Ras al Khaimah, Sharjah and Umm Al Quwain.

The Gupta brothers, Ajay, Atul and Rajesh, are believed to be in Dubai, where they own property and businesses.

They left South Africa earlier this year when Parliament called for them to be investigated for allegations of state capture.

Ajay and Atul Gupta. (Photo by Gallo Images/City Press/Muntu Vilakazi)

Multimedia · User Galleries · News in Pictures
Send us your pictures · Send us your stories

Related Links

State capture: Gordhan details meetings with the Guptas
Zondo commission: Banks subpoenaed to hand over Gupta details - report
SA and UAE sign extradition treaty

MOST READ | NEWS IN YOUR AREA | TOP LIFESTYLE

Ex-Ireland lock: Springbok World Cup win tainted by drug abuse
Guscott suggests law change to nullify Bok 'bomb squad'
Eddie Jones on where he erred in World Cup final
9 Springboks in Barbarians squad
FACT: Rassie now 'loses control' of most top Boks

More..

Read more on: guptas | parliament | politics

PH-786

Joburg Wife Turns From Rags To Riches

SM-Invest

[Photos] Meet The Spouses Of The World's Richest Billionaires

JOL

Under 65s in Eastern Cape Are Reaping Rewards Of New Life Insurance

Experts In Money Insurance

Experience the newly renovated Club Med La Pointe aux Canonniers

Club Med

This is why you should spray vinegar around your windows

Tips-and-tricks.co

Online College Degrees In South Africa - The Cost May surprise you

MBA Degrees |Sponsored Listings

More from

/News

WATCH | Shot security guard airlifted to hospital after Hurlingham house robbery

Man dies while trying to eat 50 eggs for a bet

Escalator swallows man and breaks his leg

PICS | 5 Limpopo girls die when hitching ride home…

Child electrocuted at nursery school dies in…

Shooting of top Hawks cop may affect, delay major…

Paid content

[Photos] Your Baking Soda Can Change Your Life

Healthy Gem

The Most Daring Dresses at the 2019 Met Gala

Family Minded

More from

TRAFFIC ALERTS

Western Cape

TRAFFIC

Bellville 10:59 AM

Road name: Durban Road Southbound

Southbound

Cape Town 10:35 AM

Road name: N2 Inbound

Inbound

More traffic reports traffic24

Daily Lotto: One winner on Tuesday

2019-11-12 21:18

Click here for the full list of lottery results

JOBS IN CAPE TOWN	[change area]
PROPERTY	[change area]

PH-787

6,920,992 likes

Like Page Learn More

Be the first of your friends to like this

Mom of teen shares hospital image of her daughter on life support after her lungs…

Axed Public Protector COO slams Mkhwebane: 'Bosasa, SARS rogue unit…

More from News24

Recommended by

Forget about expensive funerals

Focus on disability rights

Gymnast goes for gold in Dubai

Frisbee squad aims to grow the sport in KZN

WATCH: Lost puppy who 'fell out of the sky' turns out to be a rare purebred dingo

More severe thunderstorms, flooding expected in KZN

COMMISSION OF INQUIRY INTO STATE CAPTURE

Other Stories in South Africa...

Richard Branson apologises for all-white photo in South Africa

After a blunder in South Africa, the billionaire moved on to even more controversy in Australia.

Relative identified as person of interest in murder of Jesse Hess and her grandfather

A relative has been identified as a person of interest in the murder of Capetonian Jesse Hess and her grandfather Chris, the former University of the Western Cape student's family has confirmed.

Court instructs lawyer Tumi Mokwena to open financial books for scrutiny

The Law Society of the Northern Provinces has been granted permission to inspect all accounting records of Polokwane attorney Tumi Mokwena, following complaints of misconduct.

INSIDE NEWS24

PH-788

News24 | OLX | PROPERTY24 | CAREERS24 | SUPERBALIST | AUTOTRADER |

Potato skins are given a fun twist with a savoury egg custard and salsa.

cyberbullied cashier
"A bit of kindness goes a long way."

Sprinkles cayenne over entire life

Motshekga says parents can opt out of the LO curriculum.

S E R V I C E S

Press Code
We subscribe to the Press Code.

E-mail Newsletters
You choose what you want

News24 on Android
Get the latest from News24 on your Android device.

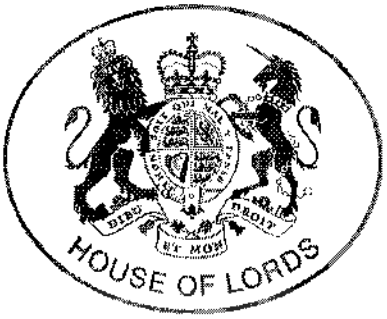
Terms and Conditions
24.com Terms and Conditions - Updated April 2012

24.com

RSS feeds · News24Wire · Search · Advertise on News24 · Jobs at 24.com · Terms & Conditions · Contact us

© 2019 24.com. All rights reserved.

iab. south africa



The Right Honourable Lord Hain of Neath
House of Lords, London SW1A 0PW

11 October 2019

Rt Hon Sajid Javid MP
Chancellor of the Exchequer
The Treasury
1 Horse Guards Parade
London SW1

Dear Sajid

Following the recent decision by the US government to impose sanctions on South Africa's Gupta business family and an associate over their role in a massive corruption and money laundering operation linked to the former president Jacob Zuma, which robbed South African taxpayers of over £500 million, I am requesting that the British government urgently does exactly the same.

Rajesh, Atul and Ajay are the Gupta brothers concerned and their South African identity numbers are listed below. I understand they currently live in at Villa L35, Lailak Street, Emirates Hills, Dubai, identifiable by the Gupta gold crest at the entrance gates and purchased with laundered funds. They also travel, including to India where they also reside and where earlier this year organised a multi-million pound wedding for two of their sons, financed by money stolen from South African taxpayers. The three are:

- GUPTA, RAJESH KUMAR, (ZA identity number: 7208056345087)
- GUPTA, ATUL KUMAR, (ZA identity number: 6806145105080)
- GUPTA, AJAY KUMAR, (ZA identity number: 6602056061184)

The financial crimes they have committed have been widely documented, including in evidence given to the Commission chaired by Judge Zondo currently investigating corruption facilitated by 'state capture' under former President Zuma.

The vast criminal network facilitated by an Indian-South African family, the Guptas and the former Presidential family, the Zumas, plundered South African taxpayer resources on an industrial scale, totally betraying Nelson Mandela's legacy and the values for which so many of us fought in the anti-apartheid struggle.

Using a network of their own companies buttressed by shadowy shell companies, the Gupta brothers obtained lucrative contracts from state owned enterprises like Eskom, Transet and South African Airways, facilitated by corrupt executives installed by former President Zuma. As a consequence the South African Revenue Service – once envied across the world for its efficiency – was nearly decimated and the state power monopoly, Eskom, bankrupted.

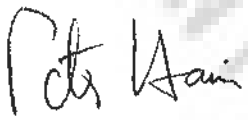
Just as the US Treasury sanctions forbids US entities from doing business with the family or handling their assets, so I ask that all UK entities are instructed to impose the same ban. These UK entities include London-based banks like HSBC, Standard Chartered and Bank of Baroda which in recent years facilitated money laundering by the Guptas and which I exposed in the House of Lords late in 2017 and early 2018.

Would you also please request the Indian and Dubai authorities to impose the same sanctions?

Over the last eighteen months South African President Cyril Ramaphosa has led the way in tackling this terrible damage and eliminating state capture, looting, cronyism and corruption. But he needs much more help from countries like Britain which have been, and may still, be conduits for the Guptas to move their criminal millions around the world.

I therefore ask you to act immediately to impose UK sanctions on the three Gupta brothers named.

Yours sincerely



Foreign & Commonwealth Office

Department for International Development

Andrew Stephenson MP
Minister of State

The Rt. Hon Lord Hain of Neath

Our ref:

05 November 2019

Dear Lord Hain,

Thank you for your letter of 11 October to the Chancellor of the Exchequer. You enquired about whether the UK planned to impose sanctions similar to those announced by the United States Department of the Treasury on 10 October against Rajesh Gupta, Atul Gupta and Ajay Gupta for money laundering and corruption in South Africa. I am replying as Minister responsible for Africa.

The US sanctions were made under their Global Magnitsky Human Rights Accountability Act. As the UK does not currently have a statutory instrument to impose sanctions for the purposes of countering corruption, we are unable to take similar measures at this stage. We are, however, pursuing other means to support the Government of South Africa in their fight against corruption.

As you will be aware, the UK Government undertakes a range of activities to tackle illicit finance, money laundering and serious and organised crime. We are engaging with the appropriate South African institutions to provide support to investigations which have a potential UK link. We are also building capacity and capability through programme activity including under the £45 million FCO-led, cross-HMG, global anti-corruption programme.

We provide funding to a number of multilateral agencies working in the Southern African region. South Africa benefits in particular from the UK's Countering Illicit Financial Flows (CIFFs) programme, which provides support to the regional asset recovery network for Southern Africa (ARINSA). ARINSA is already seeing tangible results - assets to the value of over US$500 million were seized by its members between January 2018 and March 2019.

My officials in the Africa Directorate will be in touch with your office to offer you a briefing on the detail of our activity, if that would be of interest.

Yours sincerely,

Andrew Stephenson MP

COMMISSION OF INQUIRY INTO STATE CAPTURE

Lord Peter Hain

Born in 1950 and brought up in South Africa, he has been in politics for over 50 years. His South African-born parents, Adelaine and Walter, after being jailed and then banned for their anti-apartheid activism in Pretoria were forced to leave for exile in London in March 1966 after the Government instructed all architectural firms from employing him.

Aged 19, Peter became a British anti-apartheid leader, especially in stopping all-white South African sports tours from 1969 onwards.

In December 2015 he received from South Africa the OR Tambo National Award in Silver for his 'excellent contribution to the freedom struggle'.

In 2017-18 he exposed in the UK Parliament money laundering and corruption involving global corporates on behalf of then President Zuma's family and the Gupta brothers.

In 2018 he chaired the Nelson Mandela London Centenary Exhibition Organising Committee.

In 2017 he chaired the Oliver Tambo Centenary UK Committee.

He is a Vice-President of Action for Southern Africa (ACTSA), successor to the British Anti-Apartheid Movement.

MP for Neath 1991-2015, he served in the Labour governments of Tony Blair and Gordon Brown for twelve years, seven in the Cabinet.

As Secretary of State for Northern Ireland he negotiated an end to the conflict, bringing old enemies together in government in 2007.

In November 2015 he was introduced to the House of Lords.

The author of 21 books, including *Mandela His Essential Life* (Rowman & Littlefield, 2018) his memoirs *Outside In* (London, Biteback 2012; and his parents story *Ad & Wal: values, duty, sacrifice in Apartheid South Africa* (London, Biteback, 2014.

Chairman of the Donald Woods Foundation charity, Patron of the Canon Collins Trust and a Trustee of the Liliesleaf Trust and the Listen Charity, he teaches at GIBS and Stellenbosch Business Schools and has been Visiting Professor at the University of Witwatersrand Business School.