Law Commission
Reforming the law

Anti-Money Laundering: the SARS Regime
Consultation Paper

Consultation Paper No 236

Law Commission
Reforming the law

Consultation Paper No 236

Anti-Money Laundering: the SARs Regime

Consultation Paper

20 July 2018

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

Contents

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.

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.

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]

[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.

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.

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.

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?

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?

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?

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?

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 Neil 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 Neil 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 Neil 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 Neil 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 Neil 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?

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]

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)

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”.