THE CITY LIBRARY

ISSUE 157 – JUNE 2018

COMPLIANCE OFFICER BULLETIN

The authors are lawyers in Baker McKenzie's London and US offices. They advise institutions on a broad range of financial regulatory, compliance and business crime investigations including money laundering, financial sanctions, market abuse and bribery and corruption. Baker McKenzie also represent clients in contentious financial matters including disciplinary proceedings, criminal investigations and civil litigation.

Arun Srivastava, Partner, Financial Services

Mark Simpson, Partner, Financial Services

Charles Thomson, Partner, Business Crime Unit

Jerome Tomas, Partner (US), Compliance and Investigations

Patrick M. Dennien, Associate (US) Compliance and Investigations

Henry Garfield, Senior Associate, Business Crime Unit

Richard Powell, Global PSL, Financial Services

FINANCIAL CRIME UPDATE

1 Introduction

Very little stands still for long in financial services and the same is true of financial crime. 2018 saw the implementation of the Fourth Money Laundering Directive ("4MLD"), while 2018 sees the adoption of a fifth directive ("5MLD") to strengthen its predecessor as regards customer due diligence and transparency of beneficial ownership. 5MLD, in particular, is a response by the European Commission and the Parliament to the terrorist attacks in Paris and Belgium of late 2015 and the Panama Papers scandal of 2016. Despite Brexit, we can expect these measures to be transposed into UK law given the political agreement between the UK and the EU-27 over an "implementation" period running up to 31 December 2020.

Close to the top of the government's financial crime agenda has been the Financial Action Task Force ("FATF") mutual evaluation, the site visit for which took place between February and March 2018. FATF's verdict can be expected later this year. In some respects, the UK is still conscious of the criticisms made of its anti-money laundering regime in FATF's 2007 Mutual Evaluation Report, although the 2009 Follow-up Report recognised that the UK had, in the meantime, made significant progress in remedying the deficiencies identified. To be fair, in recent years the UK has sought to place itself at the forefront of the fight against money laundering and terrorist financing, a good example being the 2016 London Anti-Corruption Summit. The 2017 National Risk Assessment nonetheless recognises that the UK's openness and status as a global financial centre exposes it to the risk of illicit financial flows and that as the risks evolve so must the response.[1]

CONTENTS

1 Introduction
2 UK AML and CTF framework: Strategy and national risk assessment
3 5MLD: What's coming; the final adopted directive
4 Financial institutions and the failure to prevent facilitation of tax evasion offences: Key implementation steps
5 Strengthening PoCA
6 Improving Suspicious Activity Reports
7 Reflections on the last six years at the UK Serious Fraud Office
8 Supervisory expectations and innovative CDD Solutions
9 The US Patriot Act Fifth Special Measure

THOMSON REUTERS™

Compliance Officer Bulletin is published by Thomson Reuters trading as Sweet & Maxwell. Thomson Reuters is registered in England & Wales, Company No.1679046. Registered Office and address for service: 5 Canada Square, Canary Wharf, London, E14 5AQ.

ISSN: 1478-1964

Compliance Officer Bulletin is published 10 times a year. Subscription prices available on request.

HOW TO PLACE YOUR ORDER

Online @
http://www.sweetandmaxwell.co.uk

By Email
TRLUKI.orders@thomson.com

By Phone
0345 600 9355 (UK)

Printed and bound in Great Britain by Hobbs the Printers Ltd, Totton, Hampshire.

This *Bulletin* will look at the implementation of not only 5MLD, but the strengthening of the Proceeds of Crime Act 2002 ("PoCA") through amendments made by the Criminal Finances Act 2017 ("CFA"), the principal vehicle for implementing the government's 2016 AML/CTF action plan. On the one hand, businesses are being required to improve their customer due diligence, while on the other, enforcement agencies are to enjoy enhanced or new powers over, for example, seizure and confiscation and unexplained wealth orders, together with the benefits of improved information sharing. Regulators and prosecutors have had their successes, for example, the Serious Fraud Office ("SFO") (in not only surviving abolition) with the use of deferred prosecution agreements ("DPA").

5MLD allows for greater control over firms and transactions involving high-risk third countries. In this context, we look at the powers of the US Financial Crimes Enforcement Network under the Patriot Act.

A discussion of how financial crime is changing cannot leave out the impact of FinTech on financial services. Nowadays, not a day goes by without publication of a new report or study. There are new phenomena such as crypto-currencies and initial coin offerings ("ICO") which present regulators with the dilemma of how to regulate them given the potential for criminality, while recognising their innovative and disruptive market tendencies. Then, there is the challenge of performing customer due diligence ("CDD") in a digital environment where the customer is present only virtually, but where technology has the potential to provide compliance solutions. Finally, there is the emergence of cybercrime which, as financial services become increasingly digital, remote and virtual, requires firms' systems and controls to be sufficiently resilient to resist attacks. Financial crime, data security, resilience and outsourcing all feature as FCA cross-sector priorities.[2]

2 UK AML and CTF framework: Strategy and national risk assessment

2.1 UK Action Plan

Two years ago, in April 2016, the Home Office and HM Treasury published the UK's action plan for anti-money laundering and counter-terrorist finance.[3] This was published at a time when financial crime, especially tax evasion and terrorist financing, was moving up the political agenda in the wake of the Mossack Fonseca scandal and, shortly before the UK's Anti-Corruption Summit. The action plan consisted of three priorities. First, to boost the powers available to law enforcement. Secondly, to improve supervision by ensuring that firms followed a risk-based approach to anti-money laundering and terrorist financing. In this respect, UK financial services were to be "the best regulated in the world". Finally, to internationalise UK efforts and extend its reach by working with the G-20 and FATF. A key element of the plan was a new "partnership" with the private sector which would see information shared between law enforcement agencies, supervisors, and the private sector. An aspect of this is the expansion of the work of the Joint Money Laundering Intelligence Taskforce, which encompasses the financial sector and law enforcement.

The plan contained a range of actions of which the CFA represents a significant part of the government's response to boosting the powers of

law enforcement to tackle money laundering. This legislation received Royal Assent in March 2017 and new powers such as over seizure and confiscation, unexplained wealth orders and improved information sharing have now been brought into force. We discuss these in more detail below. The implementation of 4MLD through the 2017 Money Laundering Regulations, on schedule last year, is viewed as bringing the UK's regime up to date with the latest international standards—the basis of 4MLD being the FATF Recommendations of 2012.

2.2 Cutting red tape

With regard to improving supervision, the government published the findings of its Cutting Red Tape review in March 2017.[4] Business had complained of a large volume of overlapping and duplicated guidance and some (but not all) viewed it as "complex, confusing and hard to understand". The interaction of the FCA's Financial Crime Guide and the JMLSG's Guidance being an example. HM Treasury is working with firms and supervisors to "streamline" AML/CFT guidance to make it clearer and less burdensome.

As for compliance, some firms complained of what they perceived as a prescriptive approach by supervisors and their fear of adverse consequences for making a mistake. As a result, businesses claimed that they were unable to act in accordance with their own risk assessments. Additionally, technological solutions were not adopted due to supervisors' preference for traditional methods. The review also noted that among the wider effects on the economy, the regime was acting as a drag on competition (e.g. a reluctance by customers to switch between different financial products) and in certain sectors there was de-risking. Another complaint concerned what was seen as a reluctance by the authorities to share information with the private sector that was reducing the regime's effectiveness at identifying and preventing wrongdoing. The CFA seeks to address this with new gateways to permit information sharing. Other areas concerned "reliance", that is the ability of one AML regulated firm to rely on the due diligence of another. Many businesses discount reliance on other firms when they remain ultimately responsible and, therefore, incur the cost of duplicating know your customer checks.

2.3 Supervision report

In March 2018, HM Treasury published an AML supervisory report for the last three years.[5] This picks up on the criticism from business of the regime by referring to the need to minimise the burden on legitimate businesses, while ensuring that the UK's financial system is "a hostile environment for illicit finance". The government believes that "effective supervision" is the key to a "successful risk-based regime that focuses supervisory and law enforcement resources on the highest risk"[6] areas. The report points to a number of important recent developments:

- FCA regulatory action and record fines for AML failings;
- a Solicitors Regulation Authority fine of £80,000 on a City of London law firm for non-compliance with the money laundering regulations;
- HMRC's a thematic review of compliance in the Money Service Business sector looking at good and bad practice; and
- collaboration between law enforcement and the accountancy sector (e.g. the Accountancy Affinity Group's development of a new risk matrix to support a consistent risk-based approach).

More specifically, in relation to AML supervisors, the UK has a large and disparate group. A total of 25 bodies. The 2015 national risk assessment found that the effectiveness of supervisors was inconsistent. On the one hand, some supervisors were not properly applying a risk-based approach to supervision and, on the other, failing to provide a credible deterrent. It is intended that the 2017 Money Laundering Regulations will clarify and strengthen expectations of these bodies. Another of the tools to raise standards among supervisors is the newly established Office for Professional Body AML Supervision that will operate under the umbrella of the FCA. Furthermore, supervisors, as do firms' nominated officers, now have the benefit of the European Supervisory Authorities guidelines on risk factors and the UK's 2017 national risk assessment. It is also the case that the 2017 Money Laundering Regulations require supervisors to provide their firms with up-to-date sector information.

As part of its report on supervision, HM Treasury has published statistics giving details of various supervisors' enforcement of the money laundering regulations over the last three years. In respect of the FCA, it will be seen that where action is taken the preferred tool is an action plan to remedy deficiencies. Fines are rare, although the cost of a s.166 report which is met by a firm might be regarded as a form of financial penalty as their cost is not insignificant.

FCA/Type of enforcement	*No. (2014/15)*	*No. (2015/16)*	*No. (2016/17)*
Action plan	23	56	72
Early interventions	8	8	7
Section 166 reports	6	6	5
Fines	1	1	3
Source: HM Treasury: AML and CTF: Supervision Report 2015/17			

2.4 UK national risk assessment

The UK's 2017 national risk assessment follows the first published in 2015. It is now a requirement of 4MLD that Member States publish such studies which regulated firms must take into account when drawing up their own business-specific risk assessments, together with similar assessments from sector supervisors. As was the case in 2015, high-end money laundering and cash-based money laundering remain the greatest areas of AML risk to the UK. By this is meant the laundering of large sums of criminal proceeds (often deriving from serious fraud or overseas corruption) through the UK's financial and professional services sectors. Additionally, it is reported that law enforcement agencies are increasingly observing "blended methodologies", as launderers attempt to use different weaknesses in different sectors. From within the UK itself, proceeds from fraud and tax offences are the principal source of criminal funds. Large remittances are another area of risk, with the report citing remittance and business links between Pakistan and the UK. The regulatory action taken by the FCA against Sonali Bank (UK) Ltd and its MLRO in October 2016 underlines the serious of this problem.[7] Other more novel sources include cyber-crime which is defined as "crimes that can be committed through the use of information communications technology devices". The report considers that while previously the risks associated with digital currencies were assessed to be low, the link between them and cyber-crime is likely to lead to the risk increasing.

Despite the initiatives taken by the government to improve the AML/CTF regime, the risk profile for financial services is not considered to have changed much recently. It is said, for example, that the banking sector continues to be vulnerable to a range of money laundering methodologies (from retail banking services as an entry point for illicit funds to complex trading arrangements being used to hide the sources of overseas funds). On the positive side, the threat is now better understood and how it varies across sectors. This is reflected in there being separate assessments for retail banking, wholesale banking and capital markets, and wealth management which also deal with correspondent banking and politically exposed persons ("PEPs"). The phenomenon of FinTech is seen positively as providing opportunities to mitigate the risk of financial crime, for instance, the role of RegTech in helping firms verify customer information.

The National Risk Assessment findings include:

- New money laundering methodologies continue to emerge.
- Use of alternative banking platforms ("ABPs") to conceal money movements in trading fraud.
- NRA assessed the banking sector to be at high risk of money laundering and at medium risk of terrorist financing.
- Poor information sharing between law enforcement and the banking sector.
- Wealth management and private banking subject to high money laundering risks due to the sector's exposure to the proceeds of political corruption and tax evasion.
- Trusts and companies used to facilitate high-end money laundering by hiding beneficial ownership.
- Likely that digital currencies are used to launder low amounts at high volume.
- Money Service Bureaux remain high risk for terrorist financing due to exposure to links to high-risk jurisdictions.

2.5 Further steps

With money laundering and terrorist financing now firmly on the public agenda, Parliament's Treasury Committee is enquiring into economic crime, looking at the AML and sanctions regimes which will include the role of financial institutions. Recommendations may result which the government will choose to implement; it recently performed a U-turn and accepted amendments to the Sanctions and Money Laundering Bill to force British overseas territories to allow access to their beneficial ownership registers by 31 December 2020.

Separately, in March 2018, the government published its response to a call for evidence over a register of beneficial owners of overseas companies and other legal entities. As a result, it is to publish draft legislation for public scrutiny this summer with a view to enacting it quickly and bringing the register into operation by 2021. This will include trusts and, for corporates, have the same definition of control used in the People with Significant Control regime. Nonetheless, the government has decided not to apply the measure to bidders for UK government contracts on the basis that it would be disproportionate to the mischief in question.

Perhaps of most significance will be the results of the FATF mutual evaluation later this year. It is likely that recommendations will be made to address any perceived deficiencies necessitating further change to the UK's regime.

3 5MLD: What is coming—the final adopted directive

5MLD has sped through the EU's legislative process, at least in relative terms. It was proposed in July 2016 and originally, it was intended to take effect as early as January 2017, that is, even before the transposition date for the 4MLD of 26 June 2017. In the event, Member States have chosen to focus on 4MLD's implementation, some of which, even then, have "missed" the transposition date. 5MLD will enter into force 20 days after publication in the Official Journal in May or June this year. Member States will then have 18 months to transpose the directive into national law—that is the end of 2019, although 5MLD also amends some of the transposition dates in 4MLD by amending art.67—for which see the various transposition dates in the table below. With respect to the establishment of beneficial ownership registers under art.30 of 4MLD, and for trusts under art.31 of 4MLD, there will in fact be an extension of time for implementation, which will help Member States that have not yet put these registers in place.

3.1 5MLD objectives

Unlike 4MLD, which completely overhauled the Third Money Laundering Directive, 5MLD will amend 4MLD in specific areas. According to the Commission its objectives are to:

- enhance the powers of EU Financial Intelligence Units ("FIUs") and facilitate their increasing transparency on the ownership of companies and trusts by establishing beneficial ownership registers;
- prevent risks associated with the use of virtual currencies for terrorist financing and limit the use of pre-paid cards;
- improve the safeguards for financial transactions associated with high-risk third countries;
- ensure centralised national bank and payment account registers or central data retrieval systems in all Member States; and
- enhance the access to information of FIUs, including in respect of the new centralised bank account registers.

We look at these changes in more detail below.

3.2 Customer due diligence and payments

The terror attacks in Paris and Belgium in 2015 were found to have been funded, in part, through the use of pre-paid payment cards. The attraction of such cards is that they are subject to lower customer due diligence standards. 5MLD is more restrictive around CDD over pre-paid cards. It also brings into AML regulation crypto currencies and exchanges. In this regard, it is worth noting that 4MLD (see Annex III)

already flags up as potentially of higher risk "products or transactions that might favour anonymity", as well as "new products and new business practices ... and the use of novel or developing technologies for both new and pre-existing products". The new measures in 5MLD include in particular:

- Pre-paid payment cards: Although it is recognised that they have a legitimate place in society, they can lend themselves to financing terrorist attacks. In amendments to art.12 of 4MLD, the scope of the exemption from performing customer due diligence in relation to pre-paid cards is to be narrowed—a card purse value of up to €250 will be reduced to €150. The current derogation permitting a Member State to increase the maximum to €500 for payment instruments in that country is abolished. Similarly, it will no longer be possible to carry out online transactions with a value of more than €50 on an anonymous basis.
- A new requirement to art.12, means that card acquirers may only accept payments carried out with anonymous prepaid cards issued in third countries where these cards meet equivalent requirements (i.e. EU due diligence standards). As a practical matter this may not be straightforward for acquirers to implement.
- Crypto (or virtual) currencies are brought within the scope of AML regulation. These are defined broadly as "a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily attached to a legal established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can transferred stored and traded electronically". The breadth of this description is just as well given recent remarks by the Mary Starks, FCA Director of Competition, to the effect that "there has been a shift from cryptocurrencies as a medium for exchange to being seen primarily as an asset class".[8] Another example, arguably, of regulation trailing technology? In any event, virtual currency exchanges, which allow virtual currencies (e.g. Bitcoin) to be converted into fiat currencies (e.g. Sterling or Euro), will be obliged entities under 4MLD and, therefore, subject to AML compliance obligations. This will allow relevant AML authorities to monitor the use of such currencies through obliged entities. The anonymity of virtual currencies is considered to give rise to the potential for misuse for criminal purposes, a reputation whether well-founded or not, that bitcoin, for example, has found difficult to dispel.
- Custodian wallet providers, that is providers of services which enable you to hold, store and transfer virtual currencies, will also be subject to regulation as obliged entities. This follows similar steps in the US. While FinTech start-ups in these areas may find their business models affected by these requirements, regulatory oversight should help to improve the confidence of other financial institutions and the public in dealing with them. Bringing both virtual currencies and custodian wallet providers into the regulatory sphere is likely to have an impact on the growing phenomena of ICOs, where the risk of money laundering and the interplay with securities law are proving to be significant hurdles. Greater assurance over anti-money laundering controls may help boost ICOs give the role played by virtual currencies.

3.3 Enhanced powers for FIS and payment accounts

4MLD enhanced the role of the FIUs and 5MLD goes further. FIUs are national entities responsible for receiving and analysing suspicious activity reports ("SARs") and other information relevant to money laundering, associated predicate offences or terrorist financing. They are tasked with making available their analyses to the relevant authorities where there are grounds to suspect money laundering offences. Consequently, FIUs play a key role, for example, in identifying the financial operations of terrorists. 5MLD increases the powers available to FIUs to access information and to be able to exchange it through appropriate co-operation with other law enforcement agencies, including those elsewhere in the EU.

In the UK, the FIU is part of, but operationally independent of, the National Crime Agency ("NCA"). The CFA amended the PoCA to give FIUs the ability, on application to court, to obtain further information from SAR reporters. This was to address the situation where SARs sometimes omit information that the FIU needs to properly analyse an activity to decide whether intervention is warranted. Moreover, on occasion, further information is necessary to build up a better intelligence picture. 5MLD now goes a stage further. FIUs will have power to obtain information from AML-regulated firms for the purposes of

preventing, detecting or combating money laundering and terrorist financing, but without the need for a prior SAR. This is discussed in this *Bulletin* below.

Even more radically, 5MLD gives FIUs (and other authorities) access to information about payment accounts (and safe deposit boxes). This refers to a new requirement on Member States to set up centralised bank account registers (or retrieval systems) to (speedily) identify holders of bank and payment accounts. Law enforcement agencies were concerned that delays to receiving this information were impeding the detection of terrorist related transfers.

What information will be available to FIUs? This will include the name of the customer and either identification data or a unique identification number, similarly for beneficial owners in the case of trust accounts and, finally, the IBAN number and date of opening and closing of the account. The concept responds to the perceived need to trace accounts and individuals rapidly. The current UK practice sees the FIU access information on payment accounts through credit reference agencies and via established contacts with account providers. The UK government considers that this works well and is likely (reluctantly) to implement a retrieval system as it is less onerous (than a centralised register) to implement and avoids the dangers of holding a large quantity of valuable information in one place. In this regard, recital 20 to the new Directive may be of help. This states that pre-existing mechanisms may be used, provided that national FIUs can access the data needed for their make inquiries in an immediate and unfiltered manner. Along with this new power, FIUs from different EU Member States will be able to co-operate with each other as well as with other authorities.

FIUs (and other authorities) are also to have a right of access to national property registers to allow for the timely identification of individuals and legal entities owning land. The Commission has until the end of 2020 to report on whether to harmonise the information held on registers and if there is a need to interconnect them. In addition to strengthening the position of FIUs, 5MLD also provides for increased co-operation between different supervisors (in particular financial services) and law enforcement authorities generally either within or between different Member States.

3.4 High-risk third countries and customer due diligence

4MLD requires the Commission to list high-risk third countries ("HRTCs") with strategic deficiencies in their AML and CTF regimes in respect of which obliged firms must carry out enhanced due diligence.[9] The approach to preparing this list has been the subject of dispute between the EU Parliament and the Commission, with the responsible Parliamentary committees rejecting an updated list in 2017. The former has been critical of the restrictive interpretation adopted by the Commission which has closely followed the lead of the Financial Action Task Force with respect to its list of high-risk and non-co-operative jurisdictions. Largely, at the instigation of the EU Parliament, the Commission will in the future and as a result of 5MLD, have to consider further elements under an amended art.9 of 4MLD. These are: (1) the availability of accurate and timely information on the beneficial ownership of legal persons and similar legal arrangements; and (2) whether there are appropriate and dissuasive sanctions, as well as the practice in those countries on co-operation and exchange of information. All this is intended to put pressure on tax havens to increase transparency.[10]

A further aspect of HRTCs centres on the Commission's concerns over the lack of uniformity in the approach that different Member States and firms take in applying EDD. In a sense, this is inherent and to be expected from a risk-based approach, the policy behind 4MLD. Under 5MLD, the Commission now seeks to harmonise checks to ensure "there are no loopholes in the EU". The new Directive therefore amends 4MLD by inserting a new art.18a to prescribe the EDD that firms must apply for business relationships or transactions involving HRTCs. The measures range from obtaining additional information to conducting enhanced monitoring of business relationships. This development is disappointing and, potentially, could lead to businesses carrying out expensive due diligence, the cost of which will ultimately be passed on to customers.

5MLD also grants the authorities the power to prohibit firms based in HRTCs from opening branches, subsidiaries or representative offices in their jurisdictions and the converse power to prohibit their firms from opening in HRTCs. Alternatively, Member States will be able to require increased supervision and external audit of such branches and subsidiaries or to insist that banks and financial services firms

terminate correspondent relationships. Of interest also is the reference in the recitals to the importance of allowing credit and financial institutions to exchange information not only between group members (which the legislation permits), but also with other credit and financial institutions subject to data protection laws. The UK, through the CFA, is already facilitating such sharing of information, provided that the NCA is informed. This is discussed further elsewhere in this *Bulletin*.

3.5 Widening access to beneficial ownership registers

4MLD required Member States to have established beneficial ownership registers for corporate entities and for trusts (when there are tax consequences) by 26 June 2017. The UK had already established a People with Significant Control Regime in 2016 which included a public register at Companies House. Transposition in the UK was therefore relatively straightforward (e.g. necessitating the range of corporate entities captured to be marginally increased).[11] The experience in other Member States has not been as straightforward and a number are still to comply (e.g. Spain). The new Directive extends the time for implementation until the end of 2019. It also widens access to beneficial ownership information. According to the Commission, this is to enhance public scrutiny and to prevent the misuse of these legal entities for money laundering and terrorist financing purposes.

With respect to corporate entities, beneficial ownership information is currently accessible to regulators, FIUs without restriction, obliged entities for the purposes of carrying out CDD and, any member of the public (as regards core information) with a legitimate interest. 5MLD removes this qualification on public access although it has not, for example, been applied in the UK. It also clarifies that tax authorities and financial sector supervisors are to have access to the register. There is provision for the supply of information in a timely manner, free of charge to the FIUs and authorities of other Member States. Where access is denied, exceptionally (because the beneficial owner might be subject to the risk of fraud, harassment etc.), this must be subject to a right of review by the courts and annual statistical information published on its use.

Firms and, where appropriate, supervisors, should report any discrepancies they find between the beneficial ownership on the register and the information available to them. According to research by NGO Global Witness more than 1 in 10 of the 4.1 million corporations registered with UK Companies House have not named "persons of significant control" although many may not have any single investor with voting rights or control in excess of 25%.

In respect of access to trusts, the changes are more significant. In addition to relevant authorities and FIUs (which now expressly include tax authorities and financial sector supervisors), those having access to the register are obliged entities—for the purposes of carrying out CDD and, any member of the public (as regards core information) with a legitimate interest. However, where a trust owns a controlling interest in an unlisted corporate entity, a member of the public does not need to demonstrate a legitimate interest to gain access.

What is a "legitimate interest" is for Member States to define according to their own national law, but it is intended to go wider than simply legal proceedings and to include investigative journalism. In a nod to privacy issues and rights to personal data, the recitals to 5MLD state that when Member States determine the level of access to beneficial information, they should have regard to the fundamental rights of individuals. There has already been a successful challenge in France by a US citizen resident in that country who had created a trust for inheritance purposes. As the disclosure in a public register of trusts showed how she intended to leave her estate, the court considered that the right to respect for her private life had been infringed and that the disclosure requirement was disproportionate to the objective of combating tax fraud and serious financial crime.[12] This decision does not mean that transparency over trusts is not possible, but it shows that such rights will need to be considered when implementing transparency measures into national law.

To help capture all relevant types of legal arrangement, Member States are to set out the characteristics of those entities which have a similar structure or function to trusts under their law. In this respect, therefore, 5MLD leaves the decision over categorisation with Member States so the risk of divergent interpretations will exist and perhaps with that some potential for arbitrage by those affected. Despite 5MLD granting greater access to the beneficial ownership of trusts, the Commission has stated its regret

that the text does not provide the same level of transparency as it does for companies and other legal entities.[13] There is some relief for those trusts which have trustees resident in more than one Member State as it will only be necessary to register in one and a certificate of registration will be sufficient proof elsewhere.

A further key development sees national registers for both corporates and trusts interconnected via the European Central Platform to facilitate co-operation and exchange of information. The Commission will take forward the necessary technical and operational issues.

In a statement of intent, the Commission considers that the specific shareholding or ownership interest threshold in 4MLD for corporates of 25%, plus one share "is merely indicative and constitutes one evidential factor among others to be taken into account".[14] Given the risk posed by non-financial entities which do not engage in an active business activity, the EU's executive suggests that obliged entities should in fact apply a lower threshold to them. This is a reminder that the Commission's original draft legislative proposal would have lowered the threshold to 10%. A substituted art.65 of 4MLD provides that, if appropriate, the Commission is to send a report to the EU Parliament and Council on the need and proportionality of reducing the threshold in the light of any (e.g. FATF) recommendation and to present a legislative proposal. More change may follow in the future.

5MLD implementation table	
Provision	*Date applies/transposition deadline*
5MLD general transposition deadline	Applies 18 months after 5MLD enters into force (i.e. the end of 2019)
Supervisors of banks and financial services firms are to reach agreement with the support of the European Supervisory Authorities on the practical modalities for the exchange of information both within and between Member States	Applies 6 months after 5MLD enters into force (i.e. the end of 2018)
Commission to assess the framework for FIU co-operation with third countries and the obstacles and opportunities	Applies by 1 June 2019
New sub-para.3 to art.12 of 4MLD: "Member States shall ensure that credit institutions and financial institutions acting as acquirers only accept payments carried out with anonymous prepaid cards issued in third countries where such cards meet requirements equivalent to those set out in paragraphs 1 and 2. Member States may decide not to accept on their territory payments carried out by using anonymous prepaid cards"	Applies 24 months after the date 5MLD enters into force (i.e. Spring 2020)
Member States must have established beneficial ownership registers for corporate entities under art.30 of 4MLD	Originally 26 June 2017. Applies within 18 months after the date of entry into force of 5MLD (i.e. the end of 2019)
Member States must have established beneficial ownership registers in respect of trusts (when the trust generates tax consequences) under art.31 of 4MLD	Originally 26 June 2017. Applies within 20 months after the date of entry into force of 5MLD (i.e. the end of 2019 or early 2020)
Member States must have established centralised automated mechanisms for accessing information on payments accounts under a new art.32a of 4MLD	Applies within 26 months after the date of entry into force of 5MLD (i.e. mid 2020)

Interconnection of registers under arts 30 and 31 of 4MLD to be completed by the Commission (with the co-operation on Member States)	Applies within 32 months after the date of entry into force of 5MLD (i.e. late 2020/early 2021). Regarding UK transposition, this may take implementation outside the "implementation period" provided for in the EU-27/UK Withdrawal agreement which expires on 31 December 2020
Commission to prepare report to EU Parliament and Council on progress under the legislation	Two years after the deadline for transposition of 5MLD (i.e. the end of 2019 and thereafter every three years)
Proposal to lower beneficial ownership test	Unspecified future date

4 Financial institutions and the failure to prevent facilitation of tax evasion offences: Key implementation steps

It is now half a year since the corporate offences of failing to prevent the facilitation of tax evasion were implemented by the CFA on 30 September 2017. These offences are on similar lines to the corporate offence of failing to have adequate procedures in relation to bribery. They also pose particular challenges for the financial services sector. Although firms were not expected to have implemented "reasonable prevention procedures" on the commencement date, they were expected to move quickly to complete initial steps, including risk assessments and implementation plans. The development of firms' procedures should now be well advanced. In what follows, we provide a recap of the main features of the regime and consider key implementation actions.

4.1 Facilitating UK and foreign tax offences

The offence of failure to prevent the facilitation of UK tax evasion can be committed by a business anywhere in the world. The only hook required for UK criminal law jurisdiction is that a taxpayer is evading a UK tax. Businesses outside the UK need to be compliant. A group subsidiary or branch located outside the UK could be guilty of a criminal offence under UK law if an employee or agent has facilitated the evasion of UK taxes. For example, a UK firm could commit an offence if an employee or agent of its Singapore branch has helped a client booked in Singapore to evade UK tax.

The foreign tax offence is narrower in scope in that it can only be committed where the offender is a UK company or partnership, the offender carries on part of its business in the UK, or any relevant conduct takes place in the UK. While HM Revenue and Customs is likely to be the main prosecutor of the UK tax offence, the Serious Fraud office will take the lead in respect of the foreign tax offence.

4.1.1 Scope of liability and relevance to financial institutions

The offences make relevant organisations criminally liable if they fail to prevent the facilitation of tax evasion by their employees and other "associated persons" (Associates). While the CFA does not impose a mandatory requirement for policies and procedures, putting these in place is recommended on the basis that doing so will provide a defence.

The extent of the procedures that are appropriate will vary widely depending on firms' risk profiles. Many financial institutions—firms which provide simple products such as consumer loans, general insurance and other non-investment products—may face comparatively low risks since their products may be less attractive to clients seeking to evade taxes. There is greater potential exposure for firms such as wealth and asset managers, as well as investment banks and other firms which manufacture bespoke investment or other financial products.

4.1.2 Liability for associates in a financial services context

An important issue is liability for Associates' conduct. Sales of financial products are often intermediated by distributors, advisers or brokers. Firms which interface directly with investors or end-clients—such as financial advisers or wealth managers—face potential liability where, for example, customer-facing staff

become aware that clients are seeking to use particular investment structures or vehicles in order to evade tax but nevertheless provide the service or product to the client.

For firms which manufacture products and sell them through a chain of intermediaries, knowing involvement by the intermediary in tax evasion by the underlying client or investor could result in liability for the product manufacturer. However, this will depend on the nature of the intermediary relationship. In many distribution chains, there may be sufficiently arm's-length relationships between independent product providers and distributors which mean that one party is unlikely to be an "Associate" of the other. However, the position may be different for agency models or where the relationship involves a degree of control.

4.1.3 Extra-territorial reach

As explained above, the CFA has extra-territorial effect. Organisations based outside the UK may choose to implement procedures where their business models expose them to material UK risk (e.g. where they deal with UK taxpayers), potentially badging any programme under a broader global tax compliance banner. UK firms' procedures should address the risk of overseas tax evasion where relevant.

4.2 Initial steps

On 1 September 2017, HMRC published its finalised Guidance on "reasonable prevention procedures". The government made clear that organisations' procedures may become more sophisticated over time, and there is a recognition that some procedures (such as training programmes and new IT systems) will take time to roll out. While this pragmatic approach provides some comfort, firms should by now have as a minimum:

- demonstrated a clear commitment to compliance by setting measures in train, including an implementation plan;
- secured top-level commitment and initial communication plan; and
- completed a risk assessment.

Although the CFA does not impose a mandatory requirement for policies to be put in place, firms should have taken these steps by now as a defensive measure. The FCA expects that firms it regulates have addressed these matters, and firms will remain subject to existing counter-financial crime obligations under the FCA Rules. We expand below on these steps and other implementation measures for financial institutions, in light of HMRC's Guidance.

4.3 The government's six principles: implementation by financial institutions

HMRC's Guidance follows six general principles. Financial services is, unsurprisingly, flagged by HMRC as a higher-risk sector.

4.3.1 Risk assessment

Any assessment of the firm's tax-specific risks should have covered off areas such as:

- product/service risk (i.e. the risk inherent in the type of product or service or the specifics of any investment structures offered, for example, the way in which investor returns are calculated or paid and the tax implications);
- client risk (i.e. risks posed by the type of client, its investment objectives and the rationale for the client's purchase of the product or service); and
- jurisdictional risks—considering where the client is located and any jurisdictions used for: (i) the domicile of investment vehicles; or (ii) the holding of assets or cash including via third-party custodians.

Associate risks: Firms should have developed a picture as to which intermediaries, consultants, product manufacturers or other third parties may constitute Associates. Firms should form a view based on the nature of the legal relationship between the firm and the relevant third party. The Guidance refers to an employee, agent or other person who performs services for or on behalf of the firm. Firms should also consider the practical risk of the relevant Associate engaging in conduct that could facilitate tax evasion.

Assessing risks is, of course, a feature of day-to-day life in a financial institution. Firms should be able to draw on their usual methodology for assessing other types of risks for their tax-specific risk assessment, and may want to consider the FCA's Financial Crime Guide, AML-related guidance such as the Joint European Supervisory Authorities ("ESAs") guidelines and the UK JMLSG Guidance.

4.3.2 Proportionality of risk-based prevention procedures

A set of procedures should be designed and practical steps should be implemented based on the outcome of the risk assessment. The Guidance makes clear that there is no need to put in place "excessively burdensome procedures" to eliminate all risk, but something "more than mere lip-service" is called for. When assessing the proportionality of any procedure the Guidance suggests firms take into account the "opportunity" available to facilitate tax evasion, what "motives" (such as reward or recognition) may be present, and the "means"; i.e., how easy would it be?

Firms should consider the following:

Policies: Whether a specific tax policy is to be developed, or whether to combine this with AML or other counter-financial crime procedures. For higher-risk firms, it may be appropriate to have a specific policy document.

Integration with existing controls: Any new procedures will need to fit alongside or within other processes/controls that firms have in place. For example, wealth managers may wish to build tax-related questions into client on-boarding documentation that is already used to comply with suitability requirements under the FCA's Conduct of Business Rules. More generally firms will want to consider alignment with AML procedures.

Guides for front office staff: Specific guidelines might be developed for client-facing staff on the questions that should be put to customers to assess tax compliance or specific "red flags" that should trigger internal escalation.

Customer agreements: From a legal perspective (as well as a compliance perspective) firms should check the language of customer agreements to consider whether existing representations and warranties are adequate or whether new tax-compliant language should be implemented.

Reporting: What processes should be in place to escalate suspicions that tax evasion is being committed or facilitated? Given that tax evasion is a predicate offence for the purposes of the Proceeds of Crime Act 2002, it would be logical to integrate this with other SAR reporting procedures. A suspicion of tax evasion may trigger a requirement to report to the NCA.

Transaction-specific mitigation measures: Firms should consider to what extent they will obtain, and place reliance on, third-party tax opinions on transactions and ensure that any such requirements are built into policies and transaction approval processes, to the extent that this is not already the case.

Project plan: Any procedural design should be accompanied by an implementation plan which sets out clear steps against a timeline for roll-out.

4.3.3 Top-level commitment

According to HMRC this was an area of priority from a timing perspective. The FCA's expectations on senior management as to financial crime risk are also relevant. Firms should address the following:

Leadership awareness: Ensure that senior management are fully briefed on the new offences and what the firm's plans are for compliance. Regular updates may be helpful.

Senior management responsibility: Firms should assign responsibility for implementation and ongoing compliance to an individual at senior level.

Internal communications: Firms should send a communication from the company's leadership/senior management to all or higher-risk staff prior last autumn. If procedures/policies have developed further communications may be relevant or more effective at a later date.

4.3.4 Due diligence

Subject to the overall risk, due diligence procedures should be applied to Associates or other third parties which have been identified as relevant during the risk assessment. Firms may consider:

Use of existing procedures: Firms are likely to have existing due diligence procedures, which cover reputational and financial issues. These procedures might not require significant adaptation—but firms should consider them through a tax-specific lens.

Specific assurance: Firms should enquire as to what their Associates have done to comply with the CFA. Firms could ask for a summary of the procedures that have been put in place and any specific risk assessment that is relevant to business done with or through the firm.

Agreements with intermediaries: Firms may want to build contractual provisions into agreements with intermediaries or other third parties, particularly where they are higher risk. Provisions may include additional representations and warranties as well as reporting, audit or other rights to enable ongoing monitoring to be done.

4.3.5 Communication and training

Firms should ensure that there is appropriate communication and training—internally and externally—where justified by the risks. In addition to any internal communications, we would expect this to involve:

External communications: Consider whether any external communication is appropriate; for example, whether any communication to intermediaries or other Associates is needed.

Training: Identify higher-risk employees and calibrate training content appropriately. Whilst the law does not require the firms' staff to become tax experts, front office staff dealing with products that are wrapped for tax purposes should be expected to have a working knowledge of relevant tax regimes, and staff dealing with customers from foreign jurisdictions might be trained on local tax regimes where relevant. In many higher-risk firms, such knowledge and awareness may well be held already. Beyond this, a basic level of training as to the CFA offences and the risks posed by non-compliance might be built in to broader compliance training given as part of staff induction and periodically.

Associates: Depending on the nature of any Associates' own internal compliance programmes, firms may decide to offer or require training by Associates.

4.3.6 Monitoring and review

Firms should put in place ongoing measures to monitor compliance and review the effectiveness of due diligence and other procedures. They should also consider building appropriate monitoring rights into contractual documentation with customers or Associates to enable future monitoring, as well as mechanisms to report potential breaches. Financial institutions' broader compliance monitoring programmes and internal audit functions can be expanded as necessary to address tax matters specifically.

5 Strengthening PoCA

The CFA is best known for introducing the corporate offences of failing to prevent the facilitation of tax evasion. The Act has, however, also strengthened PoCA by introducing or improving a number of law enforcement tools. These have recently been brought into force by secondary legislation and are now available to law enforcement agencies.

5.1 Unexplained wealth orders

The most novel power is the unexplained wealth order ("UWO"). This is a civil investigative tool which is designed to place the onus on wealthy suspects to show that their income and assets were lawfully obtained.[15] This power and the accompanying "interim freezing orders" became available on 31 January 2018. An UWO is available where:

- there is reasonable cause to believe that the respondent holds the property in question (e.g. a house) and its value is greater than £50,000;

- there are reasonable grounds for suspecting that the known sources of the respondent's lawfully obtained income are insufficient to have obtained the property; and
- there are reasonable grounds for suspecting the respondent's involvement in serious crime (or of being connected to such a person, e.g. a spouse). The test for involvement with serious crime is by reference to Part 1 of the Serious Crime Act 2007.

A prime target for UWOs is politicians or officials from outside Europe or those associated with them. In fact, where a person is a politically exposed person ("PEP"), from outside the EEA, there is no need for law enforcement agencies to suspect such a respondent's involvement in serious crime. An application is made to the High Court which will assess the matter on the civil test (i.e. the balance of probabilities). If granted, the respondent will need to explain in a statement with supporting documents, the nature and extent of their interest in the property in question and how it was obtained. It is an offence to make a false statement (or to do so recklessly). However, it is worth noting that in order to respect the rules against self-incrimination, any statement made may not generally be used in evidence against that person in criminal proceedings. If a respondent fails, without reasonable excuse, to comply, a presumption arises that the property is "recoverable property" for the purposes of Part 5 of PoCA and may be forfeited.

5.1.1 UWOs: Experience to date

Only a limited number of agencies may apply to the High Court to use UWOs. These are the NCA, HM Revenue and Customs, the Crown Prosecution Service, the Serious Fraud Office and the FCA. The NCA has been first off the mark. In February this year, it announced that it had obtained two UWOs to investigate assets of £22 million (thought to be properties) believed to be ultimately owned by a PEP. Interim freezing orders were obtained in support to prevent dissipation of these assets while the matter was investigated. The outcome of the orders is not known whether, for instance, the respondent was satisfactorily able to explain their interest. How frequently such applications will be made is unclear. The SFO has a modest annual budget (although its core funding will increase this year from £34.3 million to £52.7 million) so its capacity may be limited, but other law enforcement agencies may well step up.[16]

5.2 Seizure and forfeiture of "listed assets"

The CFA has also amended Part 5 of PoCA to enable the seizure, detention and subsequent forfeiture of "listed assets".[17] This is property that consists of precious metals (gold, silver or platinum) or stones, watches, artistic works, face-value vouchers (giving a right to goods and services) and postage stamps. The power arises in the hands of a law enforcement officer, for example, a police officer, where all (or part) of an asset is recoverable property or it is intended for use in unlawful conduct and its value is not less than £1,000.

A relevant officer may search a property for a listed asset providing they are lawfully there and have reasonable grounds for suspecting that there is a listed asset that can be seized. There are similar powers to search vehicles and indeed an individual's person, providing again there are reasonable grounds to suspect that they have a seizable listed asset. This might be an expensive watch on their wrist. A search should receive prior approval from a magistrate or, if this is not possible, from a senior officer. Following seizure, a court can order the listed asset to be further held in order to investigate its origin (or if proceedings are afoot against the person from whom it has been seized). An application may then be made to forfeit the asset. The Home Office has issued Codes of Practice under PoCA.

5.3 Further information orders

The CFA inserted ss.339ZH–339ZK into PoCA which came into force on 31 January 2018 and there are equivalent provisions in the Terrorism Act 2000 in relation to terrorist financing.[18] These new powers (which originated from FATF recommendation 29.3) allow the NCA, on behalf of the FIU, to apply to court to obtain further information over suspicions of money laundering and terrorist financing. The orders or "FIOs" are triggered by the making of a SAR under Part 7 of PoCA and can be used to obtain further information from the person who made the SAR, or from a business in the AML regulated sector. Any information disclosed as a result will not breach any restriction on the disclosure of information such as confidentiality. Alternatively, the information can be provided voluntarily. An FIO does not require a person to provide privileged information. Nor may, generally speaking, any statement provided be used

in evidence against that person under PoCA s.339ZI(1). Non-compliance with such an FIO can result in a court imposed fine of up to £5,000. Any FIO may be appealed to the Crown Court.

5.3.1 Two sets of conditions

So when would an FIO be used? To obtain one, it is necessary to satisfy one of two sets of conditions. The first is that:

- the information required relates to a matter arising from the SAR;
- the respondent made the disclosure or it is an AML regulated business;
- the information would help investigate whether a person is engaged in money laundering; and
- it is reasonable in all the circumstances to provide the information.

Alternatively, for foreign FIUs which meet the UK criteria for assistance and whose request complies with the Overseas Security and Justice Assistance Guidance, condition two requires that:

- the information relates to a matter arising which corresponds to Part 7 of PoCA (e.g. a SAR) in another jurisdiction;
- the NCA has received a request from a foreign FIU to provide information in connection with the disclosure;
- the respondent is an AML-regulated business;
- the information is likely to be of substantial value to the foreign FIU in relation their request; and
- it is reasonable in all the circumstances to provide the information.

5.4 Information sharing

One of the most significant changes to PoCA arising from the CFA is the introduction of a regime to allow firms to voluntarily share information on suspected money laundering. The Act provides a safe legal gateway for "relevant undertakings" to share information between themselves at the request of the NCA, or at the request of another firm. From 31 October 2017, banks, authorised financial services firms and professionals (such as lawyers, accountants and tax advisers) will fall within the regime.

As referred to in its action plan, the government places great store on a partnership between the private sector and law enforcement. This step is intended to secure a number of benefits, such as to enable firms to be better informed when performing due diligence and monitoring business relationships and transactions, thereby facilitating a more efficient use of finite compliance resource. However, the principal outcome intended sees better and more valuable SARs reaching the NCA.[19] These have been called "super SARs" and they exist in similar forms elsewhere in the world, for example, the US under s.314(b) of the USA Patriot Act. The concept is simple in that firms often have pieces of information which add up to make a larger picture. If they were to communicate and share their knowledge, any resulting SARs might be of better quality. It might be that a SAR would not be made where a firm had a better understanding or, conversely, one might be made where otherwise it would not. We discuss elsewhere in this *Bulletin* recent steps generally to improve the quality of SARs.

The CFA introduces new ss.339ZB–339ZG into PoCA and new ss.21CA–21CF into the Terrorism Act 2000. The voluntary sharing of information may be initiated by a firm or the NCA itself. As it is voluntary, any firm can decline to participate, but any obligation on them to make a SAR remains in force. The Home Office's published Circular, notes that a firm should consider whether they need to submit a SAR at the same time as they assess whether to share their information. One of the reasons firms may have been reluctant to make voluntary disclosures in the past was the risk of legal liability to an aggrieved client or third party. To address this concern, s.339ZF of PoCA provides that sharing information in good faith (including joint reports) does not breach any obligation of confidence owed, nor any other restriction on disclosure, however imposed. The CFA has also amended legislation on data protection to the effect, that processing personal data is "necessary", where it concerns disclosures within the regulated sector concerning a suspicion of money laundering, provided it is done in good faith. The offence of tipping off

under s.333A of PoCA is disapplied. It remains the case that where a firm has received information from a UK law enforcement agency this may not be shared without the agency's prior consent.

5.4.1 How it works

As noted above, information sharing may be instigated by a firm or the NCA itself. Where a firm, say firm "A", initiates the process (i.e. it requests another firm(s) to share information) it must notify the NCA, but need not wait for a response. All those firms involved should be mindful of their data protection responsibilities and the need to act in good faith. The requirement for good faith suggests that there must be a basis for suspecting money laundering. If the request is accepted by firm "B", firm "A" may submit a joint disclosure report on behalf of itself and firm "B" (and any further firms involved) to the NCA. Should the firms have an obligation to make a SAR this will generally be satisfied by the making of a joint report—its contents must be agreed by the MLROs of all participants. Where one or more of the firms does not make a joint disclosure report, but they continue to suspect or develop a suspicion, they must submit a SAR to the NCA as soon as is practical in the normal way. It is worth noting that if it is decided that no disclosure is needed the NCA must nevertheless be notified.

To facilitate notifications to the NCA and the making of joint reports, the existing SAR mechanism is available. Notifications should follow the NCA's guidance on SARs and should set out:

- the fact that a disclosure request has been made to another bank or authorised financial services firms;
- the firm to which the request was made;
- if known, the identity of the person suspected of money laundering with regard to the request; and
- provide all the information that would be required to make a SAR.

On receipt of the notification, the NCA will provide a case number that must be used by all the regulated firms involved when submitting information to the NCA, including any disclosure SARs, defence against money laundering SARs, notifications and joint disclosure reports.

Where it is the NCA which initiates information sharing (i.e. it suspects money laundering), it will ask firm "A" to share information with firm "B" (and possibly firm "C"). The agency will be responsible for analysing and disseminating notifications and joint disclosure reports. Firm "A" must decide if it agrees to share information with firms "B" and "C" and notify the NCA accordingly. Firms "B" and "C", may themselves decline to share, but if they do agree, they do not need to make a SAR because their obligation to do is satisfied by firm "A" notifying the NCA. As before, if a joint report does not result but a firm continues to hold their own independent suspicion they will need to make a SAR.

5.4.2 Information sharing: Will the value of disclosures improve?

How much difference super SARs will make remains to be seen and there is considerable scepticism about the utility of this gateway. The potential for improved and more valuable disclosures to the NCA can readily be seen as well as the potential for firms, armed with more intelligence, to finesse their risk-based approach to AML and CFT due diligence. The Home Office considers firms will be more prepared to disclose and share information given the benefit of added legal protection from aggrieved third parties and the risk of possible tipping-off offences. Another potential benefit, and while this might truly be an aspiration, is that better informed firms might be less inclined to de-risk potentially riskier clients: correspondent relationships and international money transfers being examples. However, the system has the potential to add complexity to AML compliance and the duties on firms' nominated officers. In the circumstances, unless the benefits are clear, regulated firms may prefer to decline to involve themselves in what is meant to be a voluntary process. Whether FCA-authorised firms will feel bold enough to turn down their own regulator—also their AML supervisor—is a moot point.

5.5 Revisiting confiscation orders

Sections 19, 20 and 21 and 22 of PoCA allow for an application to court to reconsider the grant of a confiscation order.[20] This power is relevant where new evidence, which was not originally available, comes to light. It may lead to the value of an existing confiscation order being increased to reflect the respondent having benefited to a greater extent from their criminal conduct or simply a higher sum.

In the future, due to amendments made by s.32 of the CFA to PoCA, a court will be able to reconsider the issue of confiscation for discharged orders in circumstances where there were insufficient resources to satisfy an Order or there was only a small amount outstanding. Similarly, s.33 of the Act amends Part 8 of PoCA to widen investigation powers to allow for an investigation to support such an application. This has been achieved by amending the definition of a "confiscation investigation" in s.341 of PoCA to encompass an investigation into the available amount in respect of the person, thereby supporting an application for a reconsideration of a confiscation order.

5.6 Other changes to PoCA

There have been a number of other amendments to strengthen the powers of law enforcement under PoCA. These include powers to confiscate cash in bank accounts.[21] Law enforcement agencies can now seek to freeze and subsequently forfeit funds held in bank and building society accounts that represent recoverable property or terrorist finances. Finally, and perhaps one of the most significant changes to PoCA is the extension of the moratorium period for SARs from a previous maximum of 7 days to a new maximum of 186 days.[22] This is discussed below in regard to improving SARs and what was known as the "consent regime".

6 Improving Suspicious Activity Reports

Europol's EU-wide statistics on reporting suspected criminal activity by the private sector to FIUs show that more than 65% of SARs are received by just two Member States: the UK and the Netherlands. Moreover, the UK's NCA, in its 2017 annual report, showed an increase in SARs of over 9% between October 2015 and September 2016 against the previous year. So, at first sight, the UK is ahead of Europe in the frequency of reporting by firms and the numbers of SARs it receives is increasing. This benign picture, however, hides concerns about the quality and value of UK SARs, which has caused the government to contemplate major changes. Although the most radical option was not pursued, significant reforms came into force under the CFA on 31 October 2017. Despite these steps, further reform may take place in the future.

6.1 Defence against money laundering

In the regulated sector, firms and their employees commit an offence if they fail to submit a report through a nominated officer to the NCA when they have knowledge or suspicions of money laundering or terrorist financing. This obligation is common to regulated firms in Europe under 4MLD and internationally. The UK regime differs in offering a "defence against money laundering" ("DAML") under which a reporter benefits from a defence to the primary offences of money laundering (or facilitating terrorist financing) if a transaction proceeds after a moratorium period or on receiving consent from the NCA. The very use of the term "DAML" reveals concerns by the authorities over how this regime works in practice. The previous term "consent" was being frequently misinterpreted by reporters.

The change to DAML was meant to educate reporters and improve submissions by clarifying what the UK FIU can do. Firms have sought consent to undertake transactions or activities without properly understanding the purpose of the regime. For instance, some reporters sought consent simply where they could not complete customer due diligence. The intelligence value of such SARs was nil. More generally, the regime has increased the tendency of some businesses to report defensively, with MLROs failing to consider properly if a report should be made. All this has left the authorities with a huge burden of reports of varying quality (in terms of their financial crime intelligence value) that must be investigated expeditiously and effectively.

The issues with the quality of SARs do not stop there. In September 2016, the NCA published guidance for reporters on how to request a defence in order to improve the quality SARs.[23] It was concerned that many reports were insufficiently clear and concise, and failed to provide an explicit rationale for suspicion or set out the context of the transaction. In some cases, firms could be regarded as abrogating their responsibilities and passing the buck to the NCA to take what were essentially business decisions on whether a particular transaction should proceed. The NCA warned it would take a stricter approach in closing requests where necessary information was missing or suspicions were not articulated adequately.

The UK national risk assessment into money laundering and terrorist financing of October 2015 identified a number of weaknesses and led to the government publishing and consulting in its action plan of April 2016. This included a reform of the SARs regime "through stronger partnership working between the public and private sectors, and through jointly identifying and tackling those entities—individuals, companies, and others—that pose the highest risk". The government considered the consent regime to be inefficient and proposed replacing it with an "intelligence-led approach" as consistent with the increasingly risk-based approach seen in 4MLD.

Out would go blanket consents and, instead, reporters would receive immunity for taking specified courses of action (e.g. maintaining a customer relationship when otherwise termination would alert the subject to a law enforcement investigation). The NCA would (as discussed in this *Bulletin*) also gain the power to require reporters to provide follow-up information on a SAR when needed. In light of considerable opposition from firms, the proposal to abolish the consent regime was dropped (for the time being). However, as stated in its response to the consultation, the government said it would continue to explore what could be done to prevent what it saw as the misuse of the regime.

6.2 Extended moratorium period

This has manifested itself in the reforms to the (consent or) DAML regime contained in the CFA which, for the reasons explained below, forces firms to think more clearly about whether a report is required and provides the authorities with more time to investigate potentially fewer, but more "valuable" matters. Previously, when a report was made under s.338 of PoCA, a defence was afforded to a reporter where there was no reply from the NCA after seven days. Where consent was refused, there was a further 31-day moratorium period beginning on the day of refusal (the position differs in terrorist financing cases). A reporter ran the risk of committing a money laundering offence if they proceeded with the transaction during this period. Given that these timings were generally unrealistic for any proper investigation to be carried out into the matters being reported, there was considerable incentive for firms to submit a report to benefit from the defence—against a relatively low risk of delaying the transaction beyond seven days. All this changed on 31 October 2017.

The potential moratorium period may now be extended on application to court from a maximum of 31 days to a total of 186. This means that contemplated transactions are more likely to be jeopardised by longer delays, which will increase the risk of committing a tipping-off offence. It may be relatively easy to make excuses to a client or counterparty over a delay of a week, but what about a month or longer? Additionally, in line with both the proposals in the action plan and 4MLD, the NCA now has the power to require more information following receipt of a SAR. This means that firms will need to give more thought to whether a SAR is needed and on what terms.

As referred to in the action plan, the government places great store on a partnership between the private sector and law enforcement. With that in mind (and as discussed above) the CFA makes provision for the sharing of information within the regulated sector with "Super SARs" which may produce better quality and more valuable disclosures.

6.3 Non-legislative improvements

When considering the quality of SARs and maximising their intelligence value, it should be remembered that the UK FIU has refocused its resources and structure to give a higher priority to this area. A joint SARs reform programme by the NCA and Home Office is undertaking non-legislative improvements to the operation of the regime. This includes IT and processes which, for example, aim to use SARs more intelligently (e.g. their screening for key words), to potentially fast-track priority cases to law enforcement. The NCA gives the example of SARs containing information on potential financial crimes affecting vulnerable persons. A further example is the daily checks on SARs based on key word searches following publication of the Panama Papers in April 2016.

There has also been an improvement in reporter behaviour, partly in response to published guidance and industry awareness days. One effect of this is the take-up of the best practice of using glossary codes to describe the reason a firm suspects money laundering. The NCA also cites the ability to contact reporters by email as responsible for improving the quality of subsequent requests from particular reporters.

6.4 Quantity over quality

The problem of quantity over quality remains. It is, nonetheless apparent from the NCA's last annual report that the quality of SARs is improving. This is partly through educating firms, but also through the use of new technology and the focusing of resources. The jury is nonetheless still out on the survival of the DAML regime. The government's response to its action plan consultation refers to keeping this question under review. Much will depend on whether the reforms in the CFA, now coming into force, contribute to better quality reports. It should be remembered this is a priority area for the government, with concerns over whether the UK will obtain a positive assessment from the current Financial Action Task Force's mutual evaluation, which has recently taken place. This year's NCA annual report due in July will make interesting reading.

7 Reflections on the last six years at the UK Serious Fraud Office

As David Green's tenure comes to an end, has the tanker turned? Reflections on the last six years at the UK Serious Fraud Office.

On 4 June 2018, the Attorney General announced that Lisa Osofsky will be the new Director of the SFO, taking over from David Green CB QC, who left the role in April 2018 after six years at the helm. Mark Thompson (the SFO's current Chief Operating Officer) is filling the role on an interim basis before Ms Osofsky takes up the position full time on 3 September 2018.

When referring to the SFO in a speech in 2015, David Green said that: "it is as if the oil tanker has completed its turn, and is now on the right course and making headway. The seas, of course, are always choppy if not rough for this particular tanker, and the rocks treacherous."[24] The last six years have certainly shown the seas to be rough and the rocks to be treacherous for the SFO. However, as a new Director is appointed, it is apt to consider whether David Green leaves the SFO in a better place than he found it and, as a result, whether the SFO tanker is in fact now heading in the right direction.

7.1 Historic issues

Lisa Osofsky will join an office very different to that inherited by David Green from his predecessor, Richard Alderman. By 2012, Richard Alderman's approach to self reporting and civil settlements (as opposed to criminal prosecutions) had set the scene for encouraging companies to self report their wrongdoing and to reach settlements at minimum expense to the taxpayer. Arguably, his approach was a pragmatic response to an underfunded prosecuting authority which was faced with challenging legal difficulties in holding companies liable for their wrongdoing by having to prove the directing mind and will was complicit in the fraud or bribery or corruption.

However, while having achieved some success in its early years, the SFO was facing a barrage of criticism on several fronts. Critics had no shortage of ammunition: the end of the Alderman era and the early stages of David Green's tenure were littered with controversy, criticism and setbacks.

Criticism came from a number of quarters. In 2010, Lord Justice Thomas described the $12.7 million penalty the SFO agreed to impose on *Innospec* as "wholly inadequate"[25] and the same judge further rebuked the SFO for "sheer incompetence"[26] in 2012 when it used unlawful search warrants to raid the homes and offices of property tycoons Vincent and Robert Tchenguiz while investigating the collapse of Kaupthing Bank. The investigation into the brothers subsequently collapsed and David Green was forced to issue a formal apology. In 2014, Judge Loraine-Smith roundly criticised the approach that the SFO had taken in its investigation into Victor Dahdaleh, which ultimately resulted in the trial collapsing.[27]

In its November 2012 report to the Attorney General, the Crown Prosecution Service Inspectorate found significant process failures and other weaknesses at the SFO, and that its quality of casework handling was significantly undermined by weaknesses in its systems and processes.[28]

These issues were only exacerbated by a number of high profile "out of court" incidents, including the loss of highly sensitive data in 2012, during the SFO's controversial investigation into BAE Systems plc and HMRC's fine for underpayment of VAT by the SFO. In the same period, the office was further criticised by the Parliamentary Public Accounts Committee in respect of a number of issues, including allegedly making unsanctioned severance payments to several senior employees and "showing a disregard for the proper use of taxpayers' money". [29]

Such incidents led many to question whether the organisation had a viable future as David Green took the reins.

7.2 Has the tanker turned?

Under David Green, the SFO seems to have (slowly) started to turn a corner. It now benefits from a significantly enhanced enforcement arsenal: the 2010 UK Bribery Act ("UKBA"), the introduction of DPAs, new sentencing guidelines for corporate offenders and the introduction of the new corporate tax offences in 2017 have given the SFO greater legal powers than ever before to deal with corporate offending. The SFO now also has access to "blockbuster" funding from the Treasury for larger cases and, only very recently, it was announced that its budget for the next financial year will be increased from £34.3 million to £52.7 million.[30] This additional funding will provide a much-needed boost to the office's ability to perform its role and perhaps suggests that the future of the office is more secure than had previously been the case.

There has also been a definite recalibration of the role of the SFO by David Green. His stated objective has been clear throughout his tenure: to return the SFO to its primary role as an investigator and prosecutor of "top tier" economic crime.[31] The results are stark. The SFO's investigations pipeline now reads like a who's who of blue chip UK companies across a range of industries including manufacturing, food, pharmaceutical and security. These investigations are high profile, multijurisdictional, high value and complex—precisely the types of top tier cases for which the SFO was designed 30 years ago.

7.2.1 The use of DPAs

Perhaps the most notable feature of David Green's tenure has been the coming into force of legislation permitting the SFO to enter into DPAs and the subsequent encouragement of so-called "self reporting" by companies. A DPA involves a company reaching a settlement with the SFO such that the company is charged with a criminal offence but proceedings are automatically suspended. The company also agrees to a number of conditions, which may include paying a financial penalty, paying compensation, and co-operating with future prosecutions of individuals. If the conditions are not honoured, the prosecution may resume. DPAs may be used for fraud, bribery and other economic crime. They apply to organisations, not individuals. A distinctive feature of DPAs in the UK is that they must also be sanctioned by a judge who must determine that the DPA is in the interests of justice and that its terms are fair, reasonable and proportionate.

Four DPAs have been agreed to date. On 30 November 2015, Standard Bank became the first company to enter into a DPA under which it agreed to pay a fine and compensation of $32.2 million, as well as the SFO's reasonable costs.[32] On 8 July 2016, the SFO's second DPA was agreed with a company only identified as "XYZ". XYZ was ordered to pay (along with its parent company) financial orders of £6,553,085.[33] On 17 January 2017, the SFO entered into its largest DPA to date with Rolls Royce,[34] under which Rolls Royce agreed to pay £497,252,645 plus the SFO's costs. Finally, on 10 April 2017, the SFO announced that it had entered into a DPA with Tesco who agreed to pay £285 million in financial orders in respect of certain accounting irregularities which resulted in Tesco making a £326 million overstatement of profits in 2014.[35]

7.2.2 High-profile prosecutions

David Green's SFO was also responsible for the most high-profile criminal convictions in London arising out of the global financial crisis. In August 2015, Tom Hayes was convicted and sentenced to 14 years (reduced to 11 on appeal) for his role in the manipulation of LIBOR. Convictions have also been secured of traders from other banks, while the trial of other traders is currently underway at Southwark Crown Court.

Green's tenure has also seen the first prosecutions of individuals and companies under the UKBA. Most notably, in December 2015, the Sweett Group Plc pleaded guilty to failing to prevent bribery in contravention of s.7 of the UKBA. In February 2016, Sweett Group was sentenced and ordered to pay £2.25 million.

However, David Green's tenure has not all been plain sailing. Not all prosecutions arising from the financial crisis were successful. In January 2016, six former traders were acquitted of rate manipulation, while in April 2017 the convictions of two further former traders were overturned in relation to rate rigging allegations. More recently, Tom Hayes has sought to challenge his conviction by seeking to challenge the expert evidence used to convict him.

There have also been criticisms from some quarters regarding the introduction and implementation of DPAs,[36] and convictions of large corporations for economic crime remain noticeable by their absence. Despite Green's confident assertions to the contrary, question marks clearly remain over whether the SFO can in fact get large scale, contested, multi-jurisdictional, document heavy and legally complex prosecutions of corporates over the line.

By way of example, on 21 May 2018, Barclays announced that it had been successful in dismissing charges brought against it by the SFO in June 2017.[37] Although the SFO may apply to reinstate the charges, the court's decision will undoubtedly have been a blow to David Green and the SFO, and highlights the numerous challenges that the SFO faces in prosecuting corporate entities.

During David Green's tenure, the SFO has also come under criticism for the guidance it published in June 2016, which limited the right of individuals who are summoned to an interview under the SFO's so called "section 2 powers"[38] to legal representation during the interview.[39] Commentators have been quick to question the justification for or fairness of this policy.

7.2.3 Criticism over approach

Likewise, question marks remain over the viability and/or lawfulness of the SFO's approach to investigations. Criticism of the SFO's approach to privilege has been a notable feature of Green's time in office. Green's SFO has openly sought to challenge claims to privilege that it perceives to be ill-founded and, to date, has had some success with that approach before the courts and in convincing companies subject to investigation to forego claims to privilege so as to be seen to be co-operative. However, commentators remain sceptical about the lawfulness and fairness of the SFO's approach. In *SFO v Eurasian Natural Resources Corporation Ltd*,[40] the SFO successfully challenged claims to privilege by a company over various documents that were produced by lawyers and forensic accountants during an internal investigation into allegations of bribery and corruption. The ruling, somewhat controversially, suggests that privilege (especially litigation privilege) is going to be very difficult to claim in relation to some material produced as part of an internal investigation. However, an appeal of the ENRC decision is pending, so all eyes will be on the Court of Appeal this summer when it comes to consider this controversial issue.

Several formal challenges have also been made to the SFO's procedures by way of judicial review. In 2016, Soma Oil & Gas Ltd issued judicial review proceedings to require the SFO to end its long-running investigation into potential bribery and corruption offences committed in Somalia by Soma. The proceedings were unsuccessful, but the SFO did subsequently close the investigation. In 2017, the English High Court ruled in favour of the SFO in a judicial review claim brought by Unaenergy Group Holding Pte Ltd, Unaoil Monaco SAM, Ata Ahsani, Cyrus Ahsani and Saman Ahsani. The judicial review related to the content of a letter of request sent by the SFO to the Monegasque authorities in March 2016.

More recently, the office has come under criticism following a judicial review of the way it conducted its investigation into XYZ (the unnamed company referred to above that entered into the second DPA with the SFO).[41] In particular, despite concluding that the claim had not been brought by the claimant in the proper forum, the High Court nonetheless expressed that it had "real reservations" about the SFO's decision not to procure or at least to take more active steps to obtain full interview notes from XYZ's interviews with relevant employees. Moreover, the court found that, in making that decision, the SFO had "failed to address relevant considerations, took into account irrelevant matters, provided inconsistent and inadequate reasons for its decisions, and applied an incorrect approach to the law".[42]

Another aspect of the SFO's work that continues to draw criticism is the length of time it takes to investigate matters. Investigations still take several years to complete and, as noted above, efforts by companies to challenge that time frame have failed. In particular, there are still some cases pending which were being investigated before Green took office in 2012, which seems a questionable amount of time and use of taxpayer money.

The investigation into G4S and Serco's electronic monitoring contracts is now in its fifth year, while the investigation into ENRC is almost in its sixth year. Neither of these cases appear to have progressed beyond the investigation stage.

More fundamentally, David Green's time in office has repeatedly been dogged by questions about the future of the SFO as a standalone independent investigator and prosecutor. As long ago as 2011, then Home Secretary Theresa May made clear that she favoured merging the SFO with the NCA. Although since the idea was first floated, the political drive behind it has ebbed and flowed with the broader political landscape in the UK, it is an issue that David Green has been unable to shake. What has been clear is that Green himself appears to be no fan of such a merger. By the end of the Green era, question marks about the future of the SFO appear to have quietened.

7.3 The new Director's inbox

Lisa Osofsky is currently a Managing Director, EMEA Regional Leader, and EMEA Head of Investigations of Exiger, a global compliance consultancy firm. Osofsky is a qualified English barrister, US attorney, former Deputy General Counsel and Ethics Officer of the FBI, and the former Money Laundering Reporting Officer and Executive Director of Goldman Sachs. As such, she brings a wealth of public and private sector experience from both sides of the Atlantic.

The appointment of Lisa Osofsky was certainly not expected by the white collar crime community in London, but the wealth and breadth of her experience appear to make her a good fit for the role. Observers will be especially keen to see how her background shapes the SFO's approach to its role and relations between the SFO and the US authorities in the years to come. Given her US law enforcement background, it will also be interesting to see if the new Director continues David Green's firm stance on the prosecutorial role of the SFO and to self reporting and DPAs.

Osofsky is on record as supporting plans to subsume the SFO into the UK National Crime Agency, a proposal that has been criticised by some, but welcomed by others. It will be especially interesting to see whether that is a view Osofsky maintains once she takes up the role of Director. It is difficult to predict at this stage if or how the SFO will change under new leadership. All eyes will be on their first few public speeches for a sense of the direction of travel. However, there is no doubt that the new Director will face a full inbox on their first day in the office. Surely top of their priorities will be securing convictions in the cases that are currently in court or the very significant cases due to be in court in the near future. No doubt they will also want to resolve the ongoing challenges to the SFO's procedures.

The new Director will also need to consider and implement a plan to minimise the impact of Brexit on the SFO's work, including in relation to issues such as European arrest warrants, EUROPOL membership, joint investigations, mutual legal assistance and mutual recognition of confiscation and restraint orders. If this counter-financial crime framework disintegrates post-Brexit, the SFO will need to find alternatives for facilitating international co-operation.[43]

The future of DPAs will also be interesting to track. Which company will be the next to agree a DPA with the SFO? Will we see a DPA collapse mid agreement or come unstuck? More fundamentally, observers will be keen to see whether the SFO can survive as an independent office.

7.4 Conclusions

When considered in the round, David Green leaves the SFO in a better position than he found it. Certainly Green's SFO appears to have the tools, direction and focus needed to perform its role as the principle investigator and prosecutor of complex economic crime in the UK. The tanker is clearly on the right track. However, there remains much room for improvement and much still to do before it can be said that the SFO is performing as it should. Investigations are still taking much longer than they should, funding still remains tight and question marks remain over the lawfulness and fairness of the SFO's procedures. Only time will tell if these issues can be dealt with. All eyes will be on the new Director.

8 Supervisory expectations and innovative CDD solutions

Changing technology is opening up opportunities for firms to harness new developments to help them discharge their compliance obligations. It is, nonetheless, fair to say that many compliance functions take a cautious approach, particularly with regard to the likely attitude of supervisors. For this reason, the publication earlier this year of an Opinion on the use of innovative solutions to carrying out AML/CTF customer due diligence by the three European Supervisory Authorities ("ESAs") is to be welcomed.[44] The

Opinion is aimed at national supervisors, but it is also essential reading for banks, as well as investment firms, funds, insurers and a range of other firms that are defined as "financial institutions" under 4MLD. The ESAs' supervisory expectations are also relevant to providers of online or other innovative CDD solutions.

The Opinion's content is "technology agnostic" in that it does not say what constitutes "good" or "bad" forms of "innovative" or other online CDD solutions. Instead, the ESAs want firms to be aware of the range of risks that are specific to online CDD solutions, their providers and how to put in place measures to identify, mitigate and manage those risks and, importantly for supervisors, how to evidence compliance. On this last point, it is not clear at the moment how national supervisors will embed this Opinion into the day-to-day conduct of their supervisory mandates. Firms should, however, consider updating their financial crime prevention policies, notably in respect of anti-money laundering and combating terrorist financing and their contracts with online CDD providers.

8.1 Key messages from the Opinion

So what are the key messages for firms and the principal takeaways? The Opinion sets out certain supervisory standards and expectations in respect of firms' CDD. These include the following:

- The ESAs recognise the advantages of online CDD for firms in digitising their operations but also note that that they should be mindful of how this can impact their risk exposure to money laundering and terrorist financing. It would be advisable for firms to include appropriate references in their AML/CFT policies on how risks arising from online CDD (or other potential vulnerabilities to financial crime) are to be identified, mitigated and managed.
- A re-affirmation of the existing legal and regulatory general duties (including minimum standards) to prevent financial crime. These encompass the duty to investigate/verify the identity of a customer, the purpose and intended nature of the business relationship and the obligation to monitor the business relationships and transactions on an ongoing basis, as well as the duty to verify the accuracy of information accompanying fund transfers on the basis of data, documentation or information from "reliable and independent sources".
- Firms have a degree of discretion over what constitutes "reliable and independent sources" and some flexibility over what sources of information they use to meet CDD obligations and how these correspond to what is considered at law and from other non-legislative sources to constitute "good practice". In light of the Opinion, firms should consider whether they need to review and update their current procedures.
- Confirmation that remote verification of customers' identity, based on assessing traditional identity documents and the remote verification of identity in central identity documentation databases can be beneficial if it is supported by human decision making/verification and an appropriate demonstrable "understanding and ownership" of these processes by senior management. In this respect reference is made to:
  - the importance of escalating "high-risk" customers, for example, PEPs;
  - the importance of having appropriate resources to provide a fallback to human channels in the case of system failure or the suspension/termination of online CDD services by an outsourcer. This means that firms will have to demonstrate that: (i) staff have received appropriate training; and (ii) have the technical skills necessary to oversee the development and proper implementation of online CDD, particularly where services are outsourced;
  - ensuring that senior management and compliance have a sufficient understanding of online CDD processes; and
  - ensuring that firms have in place contingency plans which will also have to be documented, but more importantly should be addressed in the firm's appropriate policies and contracts.
- A reminder to firms that their specific online CDD risks and exposure to risks arising from their CDD solutions and providers must be considered and addressed in firms' risk assessments prior to implementation. This is consistent with general obligations on using outsourced service providers as it shows despite the outsourcing, that a firm has retained sufficient oversight and control, as well as decision-making powers over CDD as a whole.

- Firms are expected to confirm to the supervisors that they have in place sufficient safeguards regarding online CDD solutions to prevent breaches of data protection and other relevant legislation. Again, firms should ensure that this is evidenced in accordance with relevant, applicable, outsourcing requirements.
- With respect to geographical risks, helpful confirmation that firms can use device fingerprinting or geolocation (on mobile devices) to assess whether a customer is located in a jurisdiction associated with higher money laundering and terrorist financing risks.
- While supervisory expectations over the "Reliability of CDD Measures" are consistent with existing communications by national supervisors, the form in which they are expressed in the Opinion may require some firms to reconsider their approach as to how they document compliance.

8.2 Supervisory expectations

The Opinion provides useful clarity over supervisory expectations on national supervisors and the firms they supervise. The majority of these expectations may require firms to review and, potentially, revise their policies, procedures and relevant contracts with third parties. The degree of the Opinion's impact on firms' approaches to CDD will vary. This will depend not only on what types of "innovative solutions" are used, but how those solutions are embedded in the firms' operations. Additionally, taking into account, how resilient they are to specific risks inherent in the solutions adopted as well as those inherent to the firm's operations and its risk exposure.

Certain types of firm may find compliance more difficult than others. For national supervisors, the ESAs expect them to co-operate, to learn from one another, and to build upon the specialist online CDD training that the ESAs plan to offer. Whilst the Opinion does not shed any light on what type of training the ESAs plan to offer national supervisors, the last sentence in para.25 is unequivocally brusque in stating: "... the ESAs consider the lack of understanding on behalf of competent authorities not to be a sufficient reason for preventing innovations and technologies from being used by firms to meet their AML/CFT obligations."

For those firms that are planning on, or those that already are, using online CDD or other innovative solutions as part of their digitisation strategies, this upskilling of supervisory approaches will be welcome. The Opinion is also likely to be of interest to a range of solution providers as they compete in establishing their regulatory compliance capabilities. As financial services intermediation and interfaces with consumers move to increased digitisation this will be a dynamic area of compliance and one seeing a range of market participants and business models. On this subject, in March 2018, UK Finance published a discussion paper entitled "Un-blocking identity in a digital world".[45] This looks at how technology could provide a solution to safely validating identity and verification and to promote discussion over the challenge of CDD in a digital economy. In particular, it looks at the use of distributed ledger technology in the financial services.

9 The US Patriot Act Fifth Special Measure

The US Financial Crimes Enforcement Network ("FinCEN"), the US anti-money laundering regulator, wields some of the most extreme powers over US financial institutions, and, by extension, the global financial system. Perhaps paramount amongst FinCEN's powers over the global financial system are its s.311 "Special Measures" powers. Although not given nearly as much fanfare as some of the other provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the Patriot Act), approximately 16 years later, these powers have grown to prominence, particularly in light of the current international economic sanctions environment. Under s.311 of the Patriot Act (31 U.S.C. 5318A) if FinCEN decides that "reasonable grounds" exist for concluding that a: (i) non-US jurisdiction; (ii) a financial institution operating in a non-US jurisdiction; (iii) one or more classes of transactions involving a non-US jurisdiction; or (iv) one or more types of accounts is a "primary money laundering concern", it may require domestic financial institutions and agencies to take certain special measures with respect to those jurisdictions, institutions, transactions, or accounts.

There are five categories of s.311 Special Measures. The first four categories permit FinCEN to impose certain additional recordkeeping, reporting, and information collection requirements upon covered US financial institutions.[46] While potentially serious, they do not on their face sever the ability of any covered

US financial institution to conduct banking transactions with the sanctioned institution or jurisdiction. However, the Fifth Special Measure does just that. Under the Fifth Special Measure, FinCEN can issue regulations prohibiting US banks from having relationships with jurisdictions or institutions deemed to be of "primary money laundering concern", effectively cutting off those jurisdictions and institutions from the US financial system.

In what follows we examine the notoriously obscure inner workings of FinCEN's decision-making process in imposing the Fifth Special Measure, as well as the effectiveness of taking such action. We also provide some observations for financial institutions looking to avoid getting caught as collateral damage.

9.1 What is the Fifth Special Measure?

Under the Fifth Special Measure, US-covered financial institutions are prohibited from opening or maintaining a correspondent account or payable through account if it involves a jurisdiction, financial institution, class of transactions, or type of account deemed to be of primary money laundering concern. US banks found to be dealing with jurisdictions of financial institutions subject to the Fifth Special Measure are liable for severe criminal and civil penalties.

Uses of the special measures are relatively rare, with only 26 rulings issued since the Patriot Act was enacted in 2001. Even then, many of the rulings overlapped and some only involving the first four special measures. FinCEN, however, has increased its use of these tools, with seven rulings issued since 2013, all involving the Fifth Special Measure.

9.2 When is it imposed?

FinCEN must make two determinations in imposing the Fifth Special Measure: (i) that a jurisdiction or institution qualifies as a primary money laundering concern; and (ii) which of the special measures will be imposed on the jurisdiction or institution.

Primary money laundering concern determination: With respect to the qualification of primary money laundering concern, FinCEN is required to consult with the Department of State and Department of Justice and consider a range of specific factors depending on whether the finding is against a jurisdiction or an institution. In deciding that a jurisdiction is a primary money laundering concern, the Treasury Secretary may look to factors including:

- whether criminal, terrorist or nuclear weapons proliferation groups have transacted business in that jurisdiction;
- whether the jurisdiction offers bank secrecy or special regulatory advantages to non-residents/non-domiciliaries of that jurisdiction, or is deemed to be an offshore banking or secrecy haven by credible groups;
- the nature and effectiveness of the bank supervisory and AML of that jurisdiction;
- the proportion of the financial transactions being effected in that jurisdiction compared to the size of its economy;
- whether the US has a mutual legal assistance treaty with that jurisdiction and experience in obtaining evidence from that jurisdiction; and
- whether it has high levels of official or institutional corruption.[47]

The factors for institutions or transactions include:

- whether criminal, terrorist or nuclear weapons proliferation groups maintain accounts or effect transactions at the institution;
- whether the institutions, transactions, or types of accounts are used for legitimate business purposes; and
- a catch-all to guard against international financial crime and money laundering.[48]

In its recent Notice of Proposed Rulemaking imposing the Fifth Special Measure against ABLV

Bank,[49] FinCEN provides examples of how it applies these criteria in practice. In that notice, FinCEN directly addressed the money laundering threat posed by ABLV Bank and the need to guard against international money laundering by taking action. FinCEN thereafter stated that ABLV Bank executives, shareholders, and employees had institutionalised money laundering as a pillar of the bank's business practices, including deliberately soliciting high-risk shell companies that enabled the bank and its customers to launder funds, maintaining inadequate controls over high-risk shell company accounts, and circumventing AML/CFT controls at the bank. According to FinCEN, these operations included transactions with sanctioned individuals and entities, some of which are involved in North Korea's procurement or export of ballistic missiles. Given this assessment, FinCEN stated also that ABLV Bank posed a national security threat, and that special measures were necessary to prevent the bank from continuing to access the US financial system.

9.3 Whether to impose the Fifth Special Measure

With respect to which special measures to be imposed, FinCEN is directed to consult with relevant agencies, including the federal functional regulators, and consider the following four factors:

(i) whether similar action has been or is being taken by other nations or multilateral groups;

(ii) whether the imposition of any particular special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organised or licensed in the US;

(iii) the extent to which the action or the timing of the action would have a significant adverse systemic impact on the international payment, clearance, and settlement system, or on legitimate business activities involving the particular jurisdiction, institution, class of transactions, or type of account; and

(iv) the effect of the action on US national security and foreign policy.

Nevertheless, FinCEN historically did not clearly disclose why it was using the Fifth Special Measure over the other tools at its disposal. While it would set out why special measures were necessary, FinCEN would not reveal why severe measures were required for the case at hand, or, conversely, why more moderate measures would not be effective.

FinCEN was forced to adapt its approach following a federal court decision in 2015. The case involved FBME Bank Ltd ("FBME")—a bank headquartered in Tanzania, but primarily doing business in Cyprus—which sought and obtained a preliminary injunction against a FinCEN final rule imposing the Fifth Special Measure.[50] As part of its decision, the Court said that it was incumbent on FinCEN to consider alternative forms to the Fifth Special Measure, which would necessarily need to be explained in its decision making. FinCEN adopted the court's rationale into its subsequent rulings, including a corrected ruling against FBME,[51] final rules for Bank of Dandong[52] and North Korea,[53] and the recent proposed rule for ABLV Bank.[54] In these rulings, the agency directly addresses whether alternative special measures would be appropriate and describes why the Fifth Special Measure is deemed necessary. In these cases, FinCEN has frequently agreed that there is no condition, additional record-keeping requirement, or reporting requirement which would be an effective measure to safeguard the US financial system against these institutions and jurisdiction. The agency argued that the targets disregarded regulatory measures designed to prevent money laundering and terrorist financing, and that no regulatory measure is sufficient to guard against a bank that processes transactions designed to obscure the underlying illicit nature or a nation that disregards international law. According to FinCEN, a prohibition against access to the US financial system through correspondent accounts and payable through accounts was the appropriate protection.

9.4 Is it effective?

There is little analysis publicly available which describes the effectiveness of the Fifth Special Measure at protecting the US financial system from money laundering and terrorist financing. FinCEN itself does not release any information on the impact or effect of such rulings, and, perhaps, may not care if the main goal is to exclude entities and jurisdictions deemed to be of "primary money laundering concern". Furthermore, it is notoriously difficult to assess the impact that a single rule or regulatory action has

had on the international transmission of criminally tainted proceeds. In fact, looking back at FinCEN's Fifth Special Measures rules, it appears that these rules have targeted similar types of jurisdictions and institutions, specifically including those which have transacted business with North Korea over the past decade.[55]

We can, however, gain some insight into the effect on the targets following several recent bouts of outrage. FBME, in its motion seeking the preliminary injunction,[56] called the ruling against it a "death sentence," and stated that it will deprive the bank of access to the US financial system and the bank will therefore "cease to exist as an international commercial bank". FBME also sharply criticised FinCEN's decision making as opaque and secretive. In December 2015, the central bank of Cyprus revoked the branch licence of FBME, forcing the bank to pull out of the country. In May 2016, the Bank of Tanzania discontinued all banking operations with FBME, revoked its banking licence, and placed it under liquidation. To date, FBME appears to continue to operate, although it is unclear in what capacity.

Similarly, the shareholders of Banca Privada d'Andorra ("BPA"), against which the Fifth Special Measure was imposed in 2015, complained in a suit against FinCEN that US banks immediately stopped doing business with BPA, making it impossible for the bank to do business in US dollars. The BPA shareholders said also that FinCEN did not provide BPA with sufficient chance to respond to the proposed ruling, and that the determination "sounded the death knell for the bank". Following the ruling, the Andorran government assumed full control of BPA and arrested its CEO on suspicion of money laundering. The Andorran government then transferred BPAs "good assets", liabilities, and clients to a new banking entity, and effectively deactivated BPA as an operational financial institution.[57]

With these two recent case studies, it is clear that there are potentially catastrophic consequences for institutions slapped with the Fifth Special Measure. While it is difficult to assess how the measures actually protected the US financial system, it is clear that the banks, with their predatory and nefarious practices, were effectively punished.

9.5 What do international financial institutions need to know?

It is important to remember that the US government has no power over overseas financial institutions. The Fifth Special Measure, as with all special measures, applies to US financial institutions. Also, the Fifth Special Measure is not an outright bar on US persons and businesses having a transactional relationship with an institution subject to these measures—the prohibition is limited to US-covered financial institutions maintaining correspondent accounts and payable through accounts for the targeted institution or jurisdiction.

US-covered financial institutions need to be diligent in the creation and oversight of correspondent accounts. As can be seen by the FBME case, non-US banks determined to be bad actors will use every trick in the book to funnel money into the US financial system. US banks should be prepared to look behind the entity holding the correspondent account to identify their ultimate beneficiaries and whether there could be any connection to the entities and jurisdictions targeted in Fifth Special Measures. The legal obligations for enhanced due diligence fall upon the US-covered financial institutions.

In practice, however, international financial institutions also need to be cognisant of the impact that these rules could have on their operations. US banks are under increased scrutiny to comply not only with the various special measures, but also more broadly those individuals and entities on the List of Specially Designated Nationals and Blocked Persons (known as the SDN List). Being able to show a clear line on the flow and source of money, as well as information on beneficial owners, will allow the correspondent banking system to move efficiently. Failure to do so may cause US-covered financial institutions (including banks) to halt or slow the transaction while they conduct their investigation, or, in extreme cases, terminate a relationship for lack of transparency. Even assuming an international bank or other financial institution maintains a state-of-the-art AML compliance programme and thus is not at risk of being hit with a Fifth Special Measures sanction, if it maintains a transactional relationship with an institution, or even a client who maintains a relationship with an institution subject to a Fifth Special Measures sanction, this will undoubtedly slow down, if not risk scuttling entirely, a transaction involving a US financial institution.

Notes

1. Home Office & HM Treasury, National Risk Assessment of Money Laundering and Terrorist Financing 2017, October 2017.
2. FCA Business Plan 2018/9. See *https://www.fca.org.uk/publication/business-plans/business-plan-2018-19.pdf* [accessed 11 May 2018].
3. Home Office & HM Treasury, Action Plan for AML and CTF, April 2016. See *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf* [accessed 14 May 2018].
4. HM Government, Cutting Red Tape, Review of UK's AML and CTF Regime, March 2017. See *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594290/anti-money-laundering-crt-red-tape-review-report.pdf* [accessed 14 May 2018].
5. Home Office & HM Treasury, AML & CTF: Supervision Report 2015–2017, March 2018. See *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685248/PU2146_AML_web.pdf* [accessed 14 May 2018].
6. Joint European Supervisory Authorities, The Risk Factors Guidelines, JC 2017 37, 26 June 2017.
7. See also NCA, National Strategic Assessment of Serious and Organised Crime, 13 May 2018 at *http://www.nationalcrimeagency.gov.uk/news/1347-national-crime-agency-publishes-2018-analysis-of-serious-and-organised-crime-threats* [accessed 15 May 2018].
8. Mary Starks, Director of Competition, FCA, Speech on Blockchain: considering the risks to consumers and competition. See *https://www.fca.org.uk/news/speeches/blockchain-considering-risks-consumers-and-competition* [accessed 30 April 2018].
9. See Commission Delegated Regulation 2016/1675. O.J. 20.9.16, L 254/1.
10. The European Commission published a first list of non-cooperative tax jurisdictions on 5 December 2017.
11. The Information about People with Significant Control (Amendment) Regulations 2017 (2017/693).
12. Décision n° 2016-591 QPC du 21 octobre 2016. See *http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-591-qpc/decision-n-2016-591-qpc-du-21-octobre-2016.148055.html* [accessed 1 May 2018].
13. I/A Item Note on Interinstitutional File: 2016/0208 (COD). See *http://data.consilium.europa.eu/doc/document/ST-8215-2018-ADD-1/en/pdf* [accessed 1 May 2018].
14. See above.
15. Home Office, Circular 03/2018: Criminal Finances Act 2017—Unexplained Wealth Orders.
16. Changes to SFO Funding. See *https://www.sfo.gov.uk/2018/04/19/changes-to-sfo-funding-arrangements/* [accessed 9 May 2018].
17. Home Office, Circular 015/2018: Criminal Finances Act 2017—Forfeiture of Property.
18. Home Office, Circular 010/2018: Criminal Finances Act 2017—Further Information Orders.
19. Home Office, Circular 007/2018: Criminal Finances Act 2017—Sharing Information within the Regulated Sector.
20. Home Office, Circular 011/2018: Criminal Finances Act 2017—Confiscation Reconsideration.
21. Home Office, Circular 005/2018: Criminal Finances Act 2017—Forfeiture of Money Held in Bank and Building Society Accounts.
22. Home Office, Circular 008/2018: Criminal Finances Act 2017: Extending the Moratorium Period for SARs.
23. NCA, Submitting A SAR within the Regulated Sector, V7.0, September 2016.
24. See *www.sfo.gov.uk/about-us/our-views/director's-speeches/speeches-2014/david-green-cb-qc-speech-to-the-pinsent-masons-regulatory-conference.aspx* [accessed 23 May 2018].
25. *R v Innospec Ltd* [2010] EW Misc 7.
26. "Judge blasts SFO over Tchenguiz case", *Financial Times*, 4 April 2012, available at *https://www.ft.com/content/a5f9b866-7e49-11e1-b20a-00144feab49a?ftcamp=published_links%2frss%2fcompanies_uk%2ffeed%2f%2fproduct%23axzz1r8wDVOqz* [accessed 23 May 2018].
27. *R v Victor Dahdelah v Mark Macdougall and Akin Gump* [2014], available at *http://res.cloudinary.com/lbresearch/image/upload/v1395768096/r_v_dahdaleh210314approvedjudgment_252114_1721.pdf* [accessed 23 May 2018].

28. HM Crown Prosecution Service Inspectorate, "Report to the Attorney General on the inspection of the Serious Fraud Office", dated November 2012, available at *https://www.justiceinspectorates.gov. uk/crown-prosecution-service/wp-content/uploads/sites/3/2014/04/SFO_Nov12_rpt.pdf* [accessed 23 May 2018].
29. House of Commons Committee of Public Accounts, "Serious Fraud Office—redundancy and severance arrangements", dated 2013-14, available at *https://publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/360/360.pdf*.
30. See *https://www.sfo.gov.uk/2018/04/19/changes-to-sfo-funding-arrangements/* [accessed 23 May 2018].
31. See *https://www.sfo.gov.uk/2013/09/02/cambridge-symposium-2013/* [accessed 23 May 2018].
32. See *https://www.sfo.gov.uk/cases/standard-bank-plc/* [accessed 23 May 2018].
33. See *https://www.sfo.gov.uk/2016/07/08/sfo-secures-second-dpa/* [accessed 23 May 2018].
34. See *https://www.sfo.gov.uk/cases/rolls-royce-plc/* [accessed 23 May 2018].
35. See https://www.sfo.gov.uk/2017/04/10/sfo-agrees-deferred-prosecution-agreement-with-tesco/ [accessed 23 May 2018].
36. See *http://www.transparency.org.uk/publications/letter-to-sfo/#.WvXtAKQvyUk*. [accessed 23 May 2018].
37. *https://www.gov.uk/government/news/new-head-of-the-serious-fraud-office-announced*.
38. Criminal Justice Act 1985 s.2.
39. See *https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/codes-and-protocols/* [accessed 23 May 2018].
40. [2017] EWHC 1017 (QB) (08 May 2017).
41. See *https://www.sfo.gov.uk/2016/07/08/sfo-secures-second-dpa/* [accessed 23 May 2018].
42. *R (on the application of AL) v SFO v XYZ Ltd, ABC LLP, MS and DJ* (at [125]).
43. See *https://parliamentlive.tv/Event/Index/4859749a-2dd8-45b9-a79c-6ef0484d655c*.
44. ESAs Opinion on the Use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process, JC 2017 81, 23 January 2018.
45. See *https://www.ukfinance.org.uk/wp-content/uploads/2018/03/WTT-Identity-Paper.pdf* [accessed 10 May 2018].
46. Covered financial institutions are defined differently for each Special Measures Regulation, but in many cases will include: insured banks, commercial banks or trust companies, savings associations, agencies or branches of foreign bank in the US, credit unions, thrift institutions; brokers or dealers in securities or commodities, mutual funds and futures commission merchants.
47. 31 USC 5318A(c)(2)(A).
48. 31 USC 5318A(c)(2)(B).
49. See 83 Fed. Reg. 33 6986 (16 February 2018), *https://www.fincen.gov/sites/default/files/federal_register_notices/2018-02-16/2018-03214.pdf* [accessed 23 May 2018].
50. See *FBME Bank v Lew*, 125 F. Supp. 3d 109, 129 (D.D.C. 2015); see also *FBME Bank v Mnuchin*, Memorandum Opinion 15 CV 01270 (D.D.C. 2015) (in later litigation on a related point, the court ruled that FinCEN had appropriately explained its rationale for relying upon SAR information as a partial basis for imposing the sanction).
51. 81 Fed. Reg. 62 (31 March 2016), *https://www.fincen.gov/sites/default/files/shared/FBME_FR_20160325.pdf* [accessed 23 May 2018].
52. 82 Fed. Reg. 215 (8 November 2017), *https://www.fincen.gov/sites/default/files/federal_register_notices/2017-07-07/2017-14026.pdf* [accessed 23 May 2018].
53. 81 Fed. Reg. 217 (9 November 2016), *https://www.fincen.gov/sites/default/files/shared/2016-27049.pdf* [accessed 23 May 2018].
54. 83 Fed. Reg. 33 6986.
55. See, Banco Delta Asia Final Rule, 72 Fed. Reg. 52,12731 *https://www.fincen.gov/sites/default/files/shared/bda_final_rule.pdf*; Bank of Dandong Final Rule, 82 Fed. Reg. 215, 51758 *https://www.fincen.gov/sites/default/files/federal_register_notices/2017-11-08/Dandong%20Final%202017-24238.pdf* [accessed 23 May 2018].

56. See Mem. Supp. Mot. Prelim. Inj., *FBME Bank v Lew*, 15 CV 1270 (CRC) (D.D.C. filed 7 August 2015).
57. See 81 Fed. Reg. 43 11648, *https://www.fincen.gov/sites/default/files/shared/BPA_Withdrawal_Finding.pdf* [accessed 23 May 2018].

Issue 158

Compiled by the Financial Services team at Norton Rose Fulbright comprising both Legal and Compliance specialists and led by Hannah Meakin, Imogen Garner, Charlotte Henry, and John Davison.

The next edition of Compliance Officer Bulletin is a MiFID II toolkit. It is designed to give you a practical overview of the key MiFID II requirements as implemented in the UK and the types of steps that firms have taken to implement them. It could be used for several different purposes including as:

- A reminder of the key MiFID II requirements.
- A signpost to where the provisions and any related guidance can be located.
- A checklist of the types of measures that firms might have taken to implement the requirements.
- A note on any issues that are under continuing discussion by the regulators or expected to the focus of their attention in coming months.
- A flag of any related legislation that should be taken into account when considering a particular topic.

It might form the basis for a post-implementation review of your compliance with the MiFID II requirements and it might help to prepare you for what the FCA might request, or expect to see, if you were asked to participate in a thematic review or supervisory visit.

The authors will cover a number of topics on both the investor protection and markets sides of MiFID II, including conflicts, best execution and inducements and transaction reporting and transparency. They will also touch on some of the more specialist regimes such as DEA, systematic internalisation, and commodity derivatives.

COMPLIANCE OFFICER BULLETIN

The regulatory environment in which financial institutions operate has been one of constant change and evolution in recent years, not only as a result of the UK regulators' own initiatives, but also as a direct consequence of the need to implement European directives within the UK, and domestic and international responses to the credit crisis.

For over 15 years, *Compliance Officer Bulletin* has been dedicated not only to aiding compliance officers to keep up to date with an unending series of changes to the UK regulatory regime, but also to providing unrivalled commentary and analysis on how FCA and PRA regulations impact on them and their business.

Published 10 times a year, *Compliance Officer Bulletin* provides in-depth, authoritative analysis of a specific regulatory area—from the complaints process to FCA investigations, money laundering to conduct of business, and from Basel to corporate governance. Each issue offers you a concise and practical resource designed to highlight key regulatory issues and to save you valuable research time.

Compliance Officer Bulletin gives you a simple way to stay abreast of developments in your profession.