THE CITY LIBRARY

ISSUE 147 – JUNE 2017

COMPLIANCE OFFICER BULLETIN

The authors are lawyers in Baker McKenzie's Financial Services Group. They advise institutions on a broad range of regulatory and financial crime-related compliance issues including insider dealing, market abuse, financial sanctions, money laundering, bribery, and corruption. Baker McKenzie's Financial Services Group also represent clients in contentious financial services matters, including disciplinary proceedings, criminal investigations (both UK and non-UK) and in civil litigation.

Arun Srivastava, Partner, Financial Services.

Mark Simpson, Senior Associate, Financial Services.

Nina Moffatt, Senior Associate, Financial Services.

Richard Powell, Professional Support Lawyer, Financial Services.

Isabel Foster, Trainee Solicitor.

FINANCIAL CRIME UPDATE

1 Introduction: All change for financial crime regulation

The next 12 months will be a busy period in the financial crime arena. While important legislative developments such as the Fourth Money Laundering Directive ("4MLD") have been in gestation for a number of years, recent events have no doubt heavily influenced the current agenda. The Panama Papers Affair has increased the focus on transparency issues and the risks arising from the use of so-called offshore tax havens. The recent spate of terrorist attacks in mainland Europe has also had an impact, particularly through the proposal for a Fifth Money Laundering Directive ("5MLD"), which also addresses issues arising from the use of technology and virtual currencies in the payments sector.

Horizon scanning: Forthcoming developments		
The Fourth Money Laundering Directive	Enhances risk-based approach to customer due diligence	Transposition date of 26 June 2017
The Fifth Money Laundering Directive	Currently in draft and subject to the trialogue legislative procedure	Likely to be adopted in summer/autumn 2017
Criminal Finances Act 2017	Firms must implement procedures to prevent the facilitation of tax offences	Likely to be in force from autumn 2017
Policing and Crime Act 2017	Increases the regulatory risk for financial sanctions breaches with new civil powers	In force from 1 April 2017 for administrative penalties for sanctions breaches

CONTENTS

1 Introduction: All change for financial crime regulation
2 4MLD and 5MLD
3 Criminal Finances Act 2017
4 Sanctions
5 FinTech and RegTech issues
6 FCA financial crime initiatives
7 Case law update: Financial crime cases from 2016/2017

THOMSON REUTERS™

Compliance Officer Bulletin is published by Thomson Reuters (Professional) UK Limited,trading as Sweet & Maxwell. 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.

Horizon scanning: Forthcoming developments		
International Tax Compliance Regulations 2015[1]	Under common reporting standards ("CRS") financial institutions must report on customers to tax authorities, with automatic information exchange with other jurisdictions	Deadline for client notification requirements over CRS related matters on 31 August 2017
Review of corporate liability for economic crime	Reform of corporate liability for economic crime generally	Feedback on consultation and legislative proposals likely for autumn 2017
UK FATF Mutual evaluation	The evaluation follows short-comings found in the UK's last FATF evaluation for AML and CTF	December 2017/early 2018

The government's implementation of the initiatives developed in its Money Laundering Action Plan[2] enacted through the Criminal Finances Act 2017 ("CFA") will create a Big Bang of change. With the UK's Financial Action Task Force ("FATF") Mutual Evaluation coming up in late 2017 or early 2018, the UK government has been keen to tighten up the UK's anti-money laundering ("AML") regime. The CFA will notably make it an offence to fail to prevent the facilitation of tax evasion. The new offence will effectively require firms who have so far been outside the "regulated sector" for money laundering purposes to introduce procedures to mitigate this risk, in much the same way that the Bribery Act 2010 required non-regulated sector firms to implement reasonable procedures to mitigate the risk of bribery. The government has also conducted a call for evidence on reform of corporate liability for economic crime generally, which may lead to the reform of the identification doctrine as regards corporate liability and/or the extension of "failure to prevent" Bribery Act-style offences to further economic crimes (e.g. fraud).

The Financial Conduct Authority ("FCA"), which is also the AML supervisor for the financial services sector, has warned in its latest Annual Business Plan[3] that where firms have poor controls, it will impose restrictions on their businesses to limit the level of AML risk and, if failings are particularly serious or repeated, it will consider prosecution. With the backdrop of continuing major enforcement action against firms for AML breaches, the FCA is striving to increase the stakes yet further by raising the spectre of criminal prosecution.

Firms must also be ready for the introduction of the 4MLD and 5MLD. As a result of 4MLD, the scope of firms subject to AML and counter-terrorist financing ("CTF") obligations has been expanded, in part through the narrowing of existing exemptions, and 4MLD also widens the definition of politically exposed persons ("PEPs") on whom

enhanced due diligence ("EDD") must be applied. Firms (as well as Member States and the European Commission itself, on behalf of the internal market) will be subject to a formal requirement to carry out and document an AML and CTF "risk assessment". 4MLD also requires the collection by companies and other legal structures (such as trusts) of information on their beneficial ownership and the storage of such information in a central register in each Member State. The UK has already largely implemented the transparency obligations under 4MLD through its domestic People with Significant Control Registers. However, the effect of the Directives will be to extend these requirements further.

The world of financial sanctions has also not been immune from change. The Policing and Crime Act 2017 gives the Office of Financial Sanctions Implementation ("OFSI") a new power to impose civil monetary penalties on transgressors, which will make taking enforcement action easier and therefore more frequent. Ahead of the Great Repeal Bill, the government is also consulting on new legislation which will allow both the sanctions and AML and CTF regimes to be maintained post-Brexit.

The new EU Market Abuse Regulation (596/2014) continues to bed down since its transposition on 3 July 2016. While we wait for enforcement cases based on the new regulation, the FCA has, for example, imposed penalties for market abuse on Tesco supermarkets for market manipulation with respect to trading statements which over stated expected profits (see Section 7, Case law update below). In another case, two individuals at Worldspreads Ltd, a spread-betting business, disseminated false and misleading information about its listed parent company and have been banned from financial services and fined for market manipulation. The two individuals were concerned in the drafting and approval of admission documents for the business' flotation that contained misleading information and omitted key information relevant to investors.[4] At the same time the FCA has continued to bring criminal prosecutions for insider dealing under Part V of the Criminal Justice Act 1993.

2 4MLD and 5MLD

The European Commission's legislative proposal for the 5MLD was published on 5 July 2016. At that time the intention was that both 4MLD and 5MLD would come into force in Member States on an accelerated timetable by the beginning of 2017. This would have been extremely challenging and common sense has prevailed, with these dates being pushed back.

The 4MLD is required to be implemented by 26 June 2017. HM Treasury consulted on 4MLD in September 2016 and feedback to the consultation was published in March alongside a draft UK Money Laundering and Transfer of Funds (Information on the Payer) Regulations ("MLR 2017") to replace the existing regulations.[5] A final version of these regulations will not now be published until after the general election on 8 June 2017 and, if they are to take effect by 26 June the government and Parliament will need to move quickly to put them in place.

5MLD is still under development. There is currently a Fifth Presidency Compromise text around which the Member States have reached a common position. The European Parliament has voted on proposed amendments to the Commission's original legislative proposal, authorising negotiations over the text with the Presidency of the Council and the Commission. The Parliament's text indicates that, if anything, it takes a harder line than the Council on due diligence requirements and transparency of beneficial ownership, no doubt due, in part, to the Panama Papers Affair which is also the subject of an EU Parliamentary investigation.[6] The affair came to light after approximately 11 million documents (2.6 terabytes of confidential information) were "leaked" from the law firm, Mossack Fonseca & Co, which acted for wealthy individuals helping them to establish offshore special purpose companies, trusts and other arrangements, which were used by some clients to evade tax. The Parliament's investigation is looking at the role played by intermediaries such as banks, law firms and accountants in obscuring the identity of ultimate beneficial owners, including poor due diligence performed by compliance officers. Among evidence heard by the committee is the central role that beneficial ownership registers have to play in combating money laundering.

2.1 Risk-based compliance

In addition to 4MLD and the MLR 2017, regulated firms will need to have regard to:

- the Commission's Supranational Risk Assessment (publication expected shortly);

- the Commission's Delegated Regulation 2016/1675 on High Risk Third Countries;[7] and
- the Joint Committee of the European Supervisory Authorities ("ESAs") Joint Guidelines on Simplified and Enhanced Due Diligence.[8]

The 4MLD develops further the risk-based approach reflected in the Third Money Laundering Directive ("3MLD"), enshrining in law a requirement for regulated firms to carry out and document the results of a risk assessment of money laundering and terrorist financing risks that they face, the results of which must be made available to regulators.

The Commission is required under art.6 of 4MLD to have carried out an assessment of the money laundering and terrorist financing facing the internal market and relating to cross-border activities by 26 June 2017.

The 4MLD also requires Member States to carry out their own risk assessments and keep those assessments up to date. HM Treasury and the Home Office published a UK Risk Assessment on 15 October 2015[9] and an update will be conducted in 2017. The results of these risk assessments must be used to inform the development of rules for each sector or area, and to be made available to regulated firms to facilitate their own risk assessments. Sector supervisors must also publish risk assessments.

2.2 What's changing?

2.2.1 Scope of regime under 4MLD

Revisions have been made to the scope of the regulated sector to capture additional types of business not currently subject to AML and CTF regulatory obligations. This includes, in particular, high-value goods dealers by lowering the amount of cash payments that a dealer must receive in order to fall within the scope of the regulated sector from €15,000 to €10,000. It now also includes dealers who not only receive but *make* such payments.

Additionally, in the gambling sector the scope of regulation now extends beyond casinos to potentially capture all "providers of gambling services". This would mean, for example, that betting shops and online betting agencies could be brought within scope. The UK has exercised the discretion given to Member States to exempt certain gambling services (in full or in part), where they assess there to be only a low risk associated with the services or on the basis of the scale of the proposed operations. This means that in the UK, apart from non-remote and remote casinos, as previously, only holders of casino operating licences will be subject to the MLR 2017.

The MLR 2017 clarify that letting agents can potentially fall within the regime as regulated entities to the extent that they carry out "estate agency work" as defined by the Estate Agents Act 1979. This is where they deal in long leases of capital value rather than all lettings agencies generally. As for estate agents they are considered to enter into a business relationship not only with (typically) the vendor but the eventual purchaser as well , therefore requiring that due diligence be undertaken.

The 4MLD also expressly includes tax crimes within the scope of predicate offences. This reflects the expanded list of predicate offences set out under the FATF Recommendations, although this amendment might be regarded as clarifying a point of principle since 3MLD's scope already included fraud and all offences punishable by maximum terms of imprisonment of more than one year (or minimum terms of imprisonment of more than six months, where applicable). In practice, tax crimes would likely have fallen within one or both categories in many jurisdictions and in the UK it is already the case that tax crimes are predicate offences under the Proceeds of Crime Act 2002 ("POCA"). All firms should be aware of the criminal corporate liability offence of failing to prevent the facilitation of tax evasion contained in the CFA that is likely to be brought into force later this year (discussed below).

2.2.2 Customer due diligence under 4MLD

One of the key challenges under 4MLD is the application of customer due diligence and in particular simplified due diligence ("SDD") and EDD. The 4MLD amends the existing due diligence framework in place under the 3MLD. In particular, a different approach is taken as to the circumstances in which SDD can be used and where EDD must be applied.

The UK's Money Laundering Regulations 2007 set out products and services in relation to which firms can apply SDD. The 4MLD takes a different approach. Instead of listing out particular products and services, it requires firms to have regard to the criteria in Annex II of the Directive in assessing whether SDD is appropriate in any given case.

In relation to SDD, the previous regime allowed a lighter-touch approach to be applied where firms took on listed companies or other regulated firms as customers (subject to equivalence requirements around the nature of the jurisdiction where the listed company or other regulated firm was based). Under the 4MLD, firms may apply such an approach where the Member State or the regulated firm itself has identified an area of lower risk, but must have regard to a series of factors set out in Annex II to 4MLD on customer risks, product/service/delivery channel risks and geographical risks. Additionally, as referred to above, the ESAs are required to develop guidelines on this issue, and in respect of which they consulted in October 2015. These provide guidance on risk assessments, methodology and risk factors, as well as sectorial guidelines.

The approach that should be taken for customer due diligence on pooled accounts has proved to be controversial, namely that SDD will be allowed only when firms providing pooled client accounts are low risk. The government continues to view pooled accounts as potentially vulnerable to money laundering. Many firms are unclear whether they will now need to perform due diligence on the beneficiaries of the funds held in a pooled account. The Law Society on behalf of solicitors considers that the position should remain unchanged (i.e. that solicitors' pooled client accounts should be considered ordinarily as low risk and eligible for SDD) as their members are required to have AML systems in place.[10]

The changes introduced by 4MLD mean that the decision whether or not to apply SDD will become more complicated. Instead of certain types of clients (e.g. publicly traded companies) or products (e.g. pooled accounts) being subject to SDD as a default position, firms will need to carry out an assessment based on the criteria listed in Annex II.

In relation to EDD, a similar approach is taken under 4MLD with firms being required to have regard to their own and national risk assessments in considering whether particular relationships are higher risk by reference to criteria set out in Annex III to 4MLD and further supervisory guidelines issued by the ESAs. Annex III to 4MLD identifies various risk factors. Of particular interest is the designation as potentially higher risk of activities such as "private banking" and "new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products". Where firms launch new products or materially amend existing products, this should act as a prompt for them to consider the associated AML and CTF risks under 4MLD.

For payments, there is an extension to the scope of circumstances in which firms are required to carry out customer due diligence. Previously, firms were required to do so when they established a business relationship or carried out an occasional transaction of €15,000 or more. Under 4MLD, customer due diligence will also be required where a transfer of funds within the scope of the revised Wire Transfer Regulation 2015/847 occurs and the amount exceeds €1,000. Regulation 2015/847 implements FATF Recommendation 16, which specifies the payer and payee information that must accompany a fund transfer for AML purposes. Payment service providers must also put in place effective procedures to spot transfers that lack this information. The ESAs are consulting on joint guidelines setting out in detail what firms must do to comply.[11]

2.2.3 High-risk countries get riskier

High-risk countries are a perennial feature of enforcement action taken against regulated firms. The recent FCA case against Sonali Bank (UK) Ltd resulted in the bank and its Money Laundering Reporting Officer ("MLRO") being fined (see below). The bank's connection with Bangladesh, a higher risk jurisdiction, was an important feature of the enforcement action taken (the bank was fined £3.25 million and the MLRO personally, £17,900).

The position of High-Risk Third Countries ("HRTCs") will become legally embedded through both 4MLD and 5MLD. The Commission's list which, takes into account FATF Public Statements and FATF's high-risk and non-cooperative jurisdictions can be a useful tool for firms. Article 9 of the 4MLD requires the EU to develop a policy towards HRTCs and 4MLD delegates powers to the Commission to issue a Regulation identifying the particular HRTC. On 3 May 2017, however, the responsible EU Parliamentary committees

rejected the latest version of the Regulation adopted by the Commission which stop the Parliament endorsed. The Parliament has criticised the list developed in the Regulation for not being far reaching enough. In particular, the Regulation does not in the Parliament's view place sufficient emphasis on jurisdictions involved with tax evasion and should not overly replicate FATF's approach.

The 5MLD also addresses the position of HRTCs. The Commission has noted that there is a lack of uniformity in the approach that the different Member States take in applying the risk-based approach. The draft 5MLD text therefore seeks to amend the 4MLD by inserting new Article 18a to prescribe the EDD that firms must apply when addressing the position of HRTCs. Interestingly, it also includes the power of competent authorities 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.

Related to country risk is correspondent banking. This is perceived to be another high-risk area that is in consequence susceptible to "de-risking" by banks. The FCA expects that UK firms which deal with non-European Economic Area ("EEA") correspondent banks must understand thoroughly the correspondent's business, reputation and the quality of its AML and CTF defences. New correspondent banking relationships must be approved by senior management.

2.2.4 Politically exposed persons

Regulation 33 of MLR 2017 requires EDD in the case of PEPs, their families and close associates. A PEP for these purposes is an individual who is, or has in the preceding year, been entrusted with a prominent public function (other than as a middle-ranking or more junior official) by a state or an international body. Immediate family members and close associates of such persons are also classed as PEPs.

The new regulations now include UK and EEA PEPs. They continue to provide that prior to entering into a relationship with a PEP, a firm's senior management must give approval to the relationship, and adequate measures together with ongoing monitoring must be taken to establish the sources of wealth and funds to be used during the relationship. New requirements have been introduced regarding life insurance business with PEPs that include a requirement for senior management to be informed before a pay-out of policy proceeds.

With the extension of the PEP regime to domestic PEPs for the first time, UK parliamentarians discovered a personal interest in its proportional application by financial institutions. This led Parliament to amend the Financial Services and Markets Act 2000 to insert a new s.333U, which requires the FCA to publish guidance on the definition of one or more categories of PEPs and to require firms "to take a proportional, risk-based and differentiated approach to conducting transactions or business relationships with each category ...". There is even a complaints and compensation scheme. The FCA is consulting on Guidance on the Treatment of PEPs under the MLR 2017.[12]

The draft FCA guidance requires authorised firms "to have appropriate risk-management systems and procedures to identify when their customer (or the beneficial owner of a customer) is a PEP and to manage the enhanced risks arising from having a relationship with that customer". Arguably, the guidance could have provided more assistance on who should be regarded as a PEP, particularly in respect of more junior office holders. Firms are reminded that they are expected to act in a proportionate manner and that there should be relatively few occasions where business relationships will need to be declined because of anti-money laundering concerns. Importantly, the guidance explains that the risks attached to each PEP will vary, giving examples of low and high risk factors and that, therefore, on a risk-based approach or "sliding-scale", the degree of due diligence needed will differ. UK PEPs should be at the lower end of the risk scale. Nonetheless, there remain concerns over the workability of the legislation which on its face still includes all MPs and members of devolved legislatives as well as members of the governing bodies of political parties (there are many registered with the Electoral Commission) and, of course, their families and close associates. Understandably, there are concerns among many firms over the amount of resource that will need to be expended to identify all PEPs and the regulatory consequences should a person pass unidentified.

The 4MLD defines "senior management" as officers/employees with sufficient knowledge of a firm's money laundering and terrorist financing exposures and sufficient seniority to take decisions affecting

risk exposure (though the Directive confirms that this does not in all cases need to be a member of the Board). This goes beyond the 3MLD position, which was not explicit and which left room for interpretation as to what constitutes "senior management". The FCA has been criticised over the absence of more guidance to firms about who in practice is to be regarded as a senior manager.

2.2.5 Joint Money Laundering Steering Group Guidance

In the light of 4MLD and the MLR 2017, the Joint Money Laundering Steering Group ("JMLSG") has consulted on revised guidance for UK firms to be in place by 26 June 2017. Both the MLR 2017 and the FCA rules provide that, when deciding whether a regulated firm has complied with the money laundering regime, regard will be had as to whether it followed the JMLSG guidance.

Helpfully, for compliance officers updating their internal policies and procedures, the JMLSG has placed a tracked changed version of their guidance on their website.[13] The sector-by-sector guidance provided by the group is invaluable in this regard. The proposed amendments include a re-ordering of the content in Ch.4 on the risk-based approach, which will be consistent with the ESAs' Risk Factor Guidelines. Chapter 5 on electronic verification has also been revised to ensure that is appropriately technology-neutral and reflects changing practice in an increasing electronic world.

Many in the industry consider that the JMLSG's guidance and the FCA's Financial Crime Guide could be "more clearly complementary and easier to understand".[14] In response, HM Treasury is to work with a reformed Money Laundering Advisory Committee to approve separate AML guidance for each sector. The new Office for Professional Body Anti-Money Laundering Supervision ("OPBAS") (discussed below) will facilitate the drafting. The intention is that this material will be complemented by the JMLSG guidance and the FCA Financial Crime Guide.

2.3 Transparency and the Panama Papers

Transparency is another key theme running through the forthcoming developments. The Panama Papers Affair has heightened concerns that offshore structures continue to be used to obscure beneficial ownership which is leading to new requirements and initiatives. A good example is the House of Lords' successful amendment to the new CFA. This requires the UK Government to prepare a report on the arrangements between the UK and Channel Islands, the Isle of Man or any British Overseas Territory for the sharing of beneficial ownership information. This is likely to maintain momentum towards encouraging those territories to improve standards of transparency. By means of an Exchange of Notes in April 2016 with the UK, the British Virgin Islands has committed to establishing and maintaining an electronic platform to store beneficial ownership information on corporate and legal entities incorporated there, which can be requested by the UK authorities but will not, otherwise, be accessible to the public. Similarly, by an Exchange of Notes, the Cayman Islands is introducing a beneficial ownership register for corporates which again while available to other authorities, will not be publicly available.

The recitals to 4MLD state that accurate and up-to-date information on beneficial owners is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. To improve transparency and reduce the misuse of legal entities, under art.30 of 4MLD, Member States must ensure that corporate entities "obtain and hold adequate, accurate and current information on their beneficial ownership" in beneficial ownership registers. These registers must be available to regulators and financial intelligence units ("FIUs") in a timely manner. Member States must also create a central register to hold this information which again must be adequate, accurate and current. In addition to regulators and FIUs, access must be available to regulated firms ("obliged entities" in the terminology used in the 4MLD) and to any other person or organisation who can demonstrate a legitimate interest. Regulators and FIUs must be able to share information with counterparts in other Member States.

Under 4MLD, beneficial ownership means "any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted ...". In the case of corporates, a shareholding of 25%, plus one share is an indication of direct ownership. Where no individual can be identified as the beneficial owner, or where there is doubt, the natural person who holds the position of senior managing official should be treated as such. The Directive exempts companies listed on regulated markets but not those listed on prescribed markets (e.g. AIM and ISDX).

2.3.1 People with Significant Control Registers

The UK has pre-empted requirements in 4MLD to establish beneficial ownership registers. The People with Significant Control ("PSC") Registers introduced in April 2016 under the Small Business, Enterprise and Employment Act 2015 (amending the Companies Act 2006), go some way towards addressing the 4MLD requirements. 4MLD includes some additional types of body corporate and requires such entities to provide updates to the central register more frequently (e.g. every six months) rather than in an annual return. The Department for Business, Energy and Industrial Strategy ("BEIS"), in its consultation on 4MLD with regard to corporate beneficial ownership, sought views on the extension of this regime to cover other types of organisations in the UK. The MLR 2017 imposes obligations in respect of beneficial ownership on a UK body corporate which is defined as "a body corporate which is incorporated or formed under the law of the United Kingdom".

Most information on the PSC Register is publicly accessible, available online and free of charge. In transposing "beneficial owner" into UK law, the government has adopted an approach consistent with the definition of "exercising significant control" for companies under the PSC regime modifying that definition as necessary in the new money laundering regulations.

The existence of a central beneficial ownership register for companies and other legal entities incorporated in Member States is likely to be of help to regulated firms carrying out customer due diligence, since the central register should be a reliable and independent source of information on the beneficial ownership of a customer. Regulated entities undertaking due diligence on beneficial ownership must record the steps they take to identify beneficial ownership. However, art.30(8) of 4MLD prevents firms from relying exclusively on the central register, and instead requires them to take a risk-based approach generally.

Currently, the principal threshold for assessing beneficial ownership is control of at least 25% of voting shares. While the Commission's original legislative proposal in 5MLD sought to lower this to 10% in line with FATF's preference, this change has been dropped from successive texts prepared by the Council of the EU although it has been maintained by the EU Parliament. It remains to be seen at what level the threshold will be agreed at when a final text is approved. A lower threshold will increase the compliance burden on firms.

2.3.2 Express trusts

In what makes a significant change for the UK, art.31 of 4MLD requires Member States to have registers of trusts administered in their respective jurisdictions. This will capture any "express trust" governed under a Member State's law and "other types of legal arrangements having a structure or functions similar to trusts". HM Treasury defines an express trust as one "deliberately created by a settlor expressly transferring property to a trustee for a valid purpose, as opposed to a statutory, resulting or constructive trust". The obligation will fall on trusts administered in the UK (and non-resident trusts with a UK source of income). As a first step, this means that trustees must obtain and hold adequate, accurate and up-to-date information on beneficial ownership including the identity of the settlor, trustees, any protector, beneficiaries (or class of) and any natural person exercising effective control. This information must be available to regulators and FIUs in a timely manner and trustees are to provide this information as a status disclosure to regulated firms when establishing business relationships.

There is also to be a central beneficial ownership register for express trusts, which in the UK is the responsibility of HM Revenue & Customs ("HMRC").[15] Trustees are to provide beneficial ownership information to HMRC on the first occasion that there is tax to declare (i.e. a return is required to declare income tax, capital gains tax and/or inheritance tax). Competent authorities and FIUs are to have timely and unrestricted access and to be able to share information with counterparts in other Member States. Member States have discretion to afford access to regulated firms for due diligence purposes, but HM Treasury states beneficial ownership information will not be shared with private entities or individuals. HMRC is to launch a register in the summer as an online service. Despite HM Treasury and HMRC attempting to minimise the burden on trustees, there is concern that the requirements on trustees to update the register at least once a year may be overly burdensome (e.g. if there is no tax to declare during any one year).

The intention of the Commission under 5MLD is that the central registers for both corporates and trusts will be interconnected via the European Central Platform. As well as specifically contemplating access to

central registers for tax authorities, the proposed Directive would also potentially allow for greater public access to central registers.

2.3.3 Overseas legal entities

In addition to the requirements of 4MLD, on 5 April 2017 the BEIS published a call for evidence on a new public register showing who controls overseas legal entities that own UK property or participate in significant UK public procurement (the "Overseas Entity Beneficial Ownership Register", or "OEBO Register").[16] The OEBO Register will be maintained by Companies House and be publicly available at no cost. Once relevant entities have provided information to the OEBO Register, they will receive a registration number which will be required in order to complete certain transactions (e.g. property transactions and public procurement).

The PSC regime has a protection regime whereby some, or all, of the information on the PSC Register can be withheld if making the information public would put the individual at risk of harm or would create a wider public safety risk. There would be a similar protection afforded to overseas legal entities.

Any regulations are far from being finalised and much will depend on their final shape. Nevertheless, if the proposals are implemented as set out in the call for evidence, they will have a significant impact on overseas organisations that hold property in the UK or frequently tender for high value UK public contracts.

The impact will be softened for entities incorporated in the EEA, though, due to the implementation of 4MLD by the end of June 2017, meaning that those entities are likely to fall within the exemption for entities incorporated in jurisdictions with equivalent disclosure regimes. Similarly, it seems likely that there will be an exemption equivalent to the PSC regime exemption for entities with voting shares admitted to trading on certain markets in Switzerland, the USA, Japan and Israel. Other overseas entities that hold property in the UK and/or frequently tender for high-value UK public contracts will face a considerable additional compliance burden. However, the government has indicated that it is sensitive to the concerns that these rules may result in a flight of investment out of the UK, and will consider carefully its economic impact with this in mind.

2.4 Supervisory authorities

In the UK, different business sectors are subject to supervision by different supervisory authorities. Regulation 7 of the MLR 2017 specifies the bodies that are responsible for the supervision of certain types of business and industry sectors. These include, for example:

- the FCA, which is responsible for the supervision of financial services firms except payment services firms which only carry out money transmission; and
- professional bodies with jurisdiction over lawyers and accountants, such as the Law Society and the Institute of Chartered Accountants in England and Wales.

In March 2017, HM Treasury announced the creation of OPBAS. This announcement derives from the Call for Information on the Anti-Money Laundering Supervisory regime of April 2016, and it is intended that this new body will help individual supervisors to fulfil their obligations, besides improving co-ordination between supervisors and law enforcement. This is in the light of concerns that the quality of supervision across sector supervisors has not been all that it should, leading to uneven regulation. The OPBAS is to be situated within the FCA, which is to be responsible for reviewing the quality of AML supervision carried out by professional bodies such as the Solicitors Regulation Authority and the Institute of Chartered Accountants in England and Wales. It is intended to be operating from early 2018. One of the objectives of the Call for Information was to cut red tape; however, there is a risk that this additional supervisor will simply add to its weight.

3 Criminal Finances Act 2017

The CFA was granted Royal Assent on 27 April 2017 and the Act's substantive provisions are likely to be brought into force later this year or next. It is in large part the legislative response to the Home Office and HM Treasury's Action Plan for Anti-Money laundering and Counter-terrorist Finance (Money Laundering Action Plan).[17]

3.1 Action Plan for Anti-Money Laundering and Counter-Terrorist Finance

The Money Laundering Action Plan published in April 2016 contained proposals to overhaul the UK's AML and CTF framework that represented significant changes. It focused in particular on money laundering as an enabler of serious organised crime, grand corruption and terrorism. It addressed four policy priorities:

3.1.1 To create a stronger partnership with the private sector

This would see agencies, supervisors and private entities partnering to target their resources at the highest risks (rather than the lowest as frequently occurs), introducing new ways of sharing information and adopting a collaborative approach to prevent individuals becoming involved in laundering activities. In this respect, the government wanted to improve the suspicious activity reporting ("SAR") regime and even considered abolishing the consent regime.

There were a number of concerns underlying this. It has increased the tendency of some businesses to report defensively, where MLROs fail to consider properly if a report should be made. SARs can be poor quality and reports abrogate responsibility for essentially commercial decisions on whether to proceed with a client or report a transaction to the National Crime Agency ("NCA"). In addition to this, the current moratorium period of 30 days does not give law enforcement sufficient time to properly investigate SARs before taking a decision to grant a consent or not.

Instead, it was contemplated that, in future, those reporting suspicious activity might instead be granted immunity for taking specified courses of action. The government gave the example of maintaining a customer relationship when its termination would tip off the subject about an investigation. This option was not in the event pursued in the light of opposition from firms.

3.1.2 To strengthen law enforcement responses to AML and CTF threats

There may be a grant of additional powers to those already in POCA. A number of examples were cited including administrative powers that other countries use to disrupt money launderers. Asset recovery provisions could be strengthened to allow law enforcement agencies to forfeit the proceeds of crime held in bank accounts. Additionally, there was scope to improve financial investigation powers. The adoption of new capabilities is exemplified by the government's establishment of a Joint Task Force of the NCA and HMRC to investigate possible illegality relating to the data released from Mossack Fonseca & Co, the law firm based in Panama.

3.1.3 To reform the supervisory regime

The effectiveness of the current supervisory regime and options for improvement were considered with a view to ensuring that a risk-based approach is fully in place. This would necessitate moving away from a "tick box" approach to compliance towards an understanding of specific risks and an ability to the spot criminal activity. As referred to above, the government announced in March 2017 the creation of OPBAS, which will work with professional supervisory bodies to help them meet their obligations.

3.1.4 To increase the UK's international reach to tackle money laundering and terrorist financing

The UK is to collaborate with the G20, FATF and other international groups to achieve better co-operation with key jurisdictions. A specific example is the proposal to increase the provision of beneficial ownership information by foreign companies investing in the UK on which (as discussed) the BEIS is consulting.

3.2 "Failure to prevent" corporate liability offences

The most significant development in the CFA is the new corporate offences of failing to prevent the facilitation of tax evasion. The possibility of extending the Bribery Act 2010 to a wider range of economic crimes was announced at the time of the UK's Anti-Corruption Summit in May 2016. The concept is to make a company or a firm criminally liable for the acts of its employees, agents or other associates where they have facilitated another person to evade the payment of tax. It is strict liability, meaning that the company can be made criminally liable even though the corporate mind (typically the directors and other senior management) did not know of or were not involved in the relevant conduct. In structure it is similar to the corporate failure to prevent offence under the Bribery Act 2010, in that a firm will have a defence if it can show that it had reasonable internal procedures in place to prevent the conduct concerned from occurring (or it was reasonable not to have such procedures).

This means that firms will need to develop policies which specifically address the risk of tax evasion. Draft guidance on what firms need to do by way of procedures has been produced by the HMRC.[18] This contains a number of helpful worked examples.

The Act creates two new offences for corporates which fail to prevent their staff facilitating evasion of both UK and foreign taxes. The jurisdictional reach of the offences is extremely broad:

- the offence of facilitating the evasion of a UK tax can be committed by anyone and anywhere in the world. The fact that the conduct concerned took place outside the UK is irrelevant. The UK authorities would, of course, encounter problems enforcing this where the persons concerned are located abroad; and
- the offence of facilitating the evasion of a foreign tax can be committed by: (1) a UK headquartered business; (2) a person who carries on part of their business in the UK; or (3) where any part of the conduct occurs in the UK.

3.2.1 Do I need to become a tax expert?

It is frequently asked whether the new offences means that businesses and their employees need to become experts in tax laws around the world to avoid committing an offence. The answer to this is "No", it is not necessary to develop expertise in all taxes around the world. The idea behind the offence is not to capture inadvertent offences, but rather to target deliberate facilitation of criminal tax evasion.

Having said that, it is important for firms to carry out a risk assessment and understand where risks in their business lie in relation to the potential to facilitate tax evasion.

3.2.2 Are there other reasons to be concerned?

While firms may be relieved to know that they do not need to become tax experts, the very broad reach of the offences means that firms with an international presence will need to consider the position carefully. In particular:

- Your overseas branches or subsidiaries could commit the offence as it captures conduct engaged in anywhere in the world. For example, your Singapore branch advising a UK expat client could commit the offence by facilitating that person's evasion of a UK tax.
- If you are based in the UK, the question is: what expectations and responsibilities will be placed on you in relation to such conduct? The offence of facilitating the evasion of a foreign tax can be committed by a UK company anywhere in the world. Therefore, your New York office could commit the offence in relation to conduct engaged in New York that facilitates the evasion of a US tax, because the legal entity concerned is a UK company.
- The foreign offence might also be committed in relation to conduct engaged in entirely outside the UK. For example, a Cayman partnership or company which facilitates the evasion of US taxes from the Cayman Islands could be guilty under UK law if it carries on part of its business in the UK (i.e. it can be any part of the business in the UK and not the business involved in the facilitation of the tax evasion).

It is clear from this that firms need to take an expansive approach to the policies and procedures they put in place making sure all relevant jurisdictions are covered.

And what is more, on 13 January 2017, the Ministry of Justice launched a Call for Evidence on corporate liability for economic crime.[19] The government is looking at four options to reform "the identification doctrine" governing corporate liability for certain crimes. These are:

- reforming the identification doctrine (i.e. broadening the scope of those considered to be the directing mind of a company);
- introducing a strict liability offence based on the principles of vicarious liability as in the US; or alternatively
- a corporate liability offence deriving from the responsibility of a company to ensure that offences are not committed on its behalf; and
- a failure to prevent offence on the lines of the Bribery Act.

Judged by the amount of space dedicated to discussing these options, the last is the front runner. In the light of recent deferred prosecution agreements ("DPAs"), the government considers that the corporate failure to prevent offence under the Bribery Act 2010 has been a success and could be extended to other crimes such as fraud, false accounting and money laundering. A consultation is promised if this option (as seems likely) is pursued. Incidentally, backbench Members of Parliament attempted to amend the CFA during its parliamentary passage to add a failure to prevent economic crime offence. It is likely that such an offence could be included in legislation introduced in the next parliamentary session after the general election. One caveat for financial services is that the government may conclude that the corporate failure to prevent offence is unnecessary in the financial sector given the new rules on individual responsibility under the Senior Managers Regime (which are due to be extended to all firms in 2018).

These new offences must be seen in the context of the introduction of Common Reporting Standards from 2017/2018 with the automatic exchange of financial information between tax authorities in over 90 countries (e.g. with Crown Dependencies and UK Overseas Territories), which is another important factor in the prevention of tax evasion. The UK government is also introducing tougher civil penalties for offshore tax evasion and removing the need to prove intent in the most serious cases of failing to declare offshore income and capital gains.[20]

3.3 Other reforms under the Criminal Finances Act

3.3.1 Consent regime reform

The government, having decided against more radical reforms has, through the vehicle of the CFA, extended the moratorium period in the consent regime. The regime in respect of money laundering is contained in s.335 of POCA (in respect of counter-terrorism at s.21ZA of the Terrorism Act 2000). The regime, which has few equivalents internationally, brings a number of benefits. For example, it incentivises businesses (including unregulated businesses) to report by providing a defence to the primary offences of money laundering (or facilitating terrorist financing) where the transaction proceeds, while providing the authorities with an opportunity to investigate.

Under the CFA, POCA will be amended to give law enforcement a moratorium period of up to 186 days. This will allow law enforcement to have sufficient time to investigate the matters being reported. However, for firms a lengthy extension of the moratorium period will mean that they are more likely to be trapped between a rock and a hard place, between their client and the NCA. Law enforcement will need to go to court to get an order extending the moratorium period. In this process they will need to show that they have been investigating matters expeditiously.

3.3.2 Unexplained wealth orders

The CFA amends POCA to introduce a new tool for enforcement agencies as recommended by the Money Laundering Action Plan. The introduction of unexplained wealth orders ("UWOs") addresses the position of individuals whose wealth is disproportionate to their income. Such orders are already used in some other jurisdictions, such as Ireland and Australia. In part, they will address the difficulty that the UK authorities often face in achieving co-operation from overseas jurisdictions to obtain evidence of wrongdoing.

The CFA gives law enforcement the power to obtain an order from the High Court requiring certain persons to provide an explanation of their wealth. Such an order can only be obtained against PEPs or a person suspected of serious crime. The government's impact assessment estimates there will be 20 cases per year after the first year of operation. The power is relevant to where individuals are involved in corruption overseas (catching foreign PEPs), or in serious crime in the UK, and is particularly useful where law enforcement do not have sufficient evidence. Financial institutions which provide financial and banking services to individuals made subject to such orders may have cause to review their know your customer procedures, lest the authorities consider that they are indicative of failings or weaknesses in their AML and CTF systems and controls.

More specifically, the High Court can require a respondent, who may be a person outside of the UK, to provide an explanation of the nature and extent of their interest in specified property (which has a £50,000 *de minimis* threshold), how it was obtained, and how the costs of acquiring the property were met.

The UWO may also require the respondent to disclose specified information or documents. To be granted a UWO, the applicant must satisfy the court that there are reasonable grounds for suspecting that the respondent's known sources of lawful income would have been insufficient to enable the respondent to obtain the property.

Additionally, the court must be satisfied that either: (i) the respondent is a PEP; or (ii) there are reasonable grounds for suspecting that they are or have been involved in (or are connected to someone who is or has been involved in) serious crime in the UK or elsewhere. Any respondent who is unable to comply with a UWO risks having their assets seized, as the CFA creates a presumption that such property with unexplained financial origins amounts to "recoverable property" within the civil recovery powers in Pt 5 of POCA.

The UWO regime holds PEPs to a much higher standard. The High Court could grant a UWO against a PEP simply by virtue of reasonable grounds of suspicion that their known sources of lawful income would have been insufficient to enable the respondent to obtain the property, without any requirement for a reasonable belief that they (or someone connected to them) are involved in criminality. That said, on the face of these powers, a UWO certainly provides a strong disincentive to those who would seek to acquire UK property with criminal funds. However, given the apparent high test that must be satisfied for non-politically exposed persons before a UWO will be granted, it remains to be seen whether UWOs will be used as an investigatory tool in the armoury against complex financial crime, or simply as a final step in the civil recovery of the proceeds of suspected criminality.

3.3.3 Extended seizure and forfeiture powers

The CFA boosts enforcement authorities' powers of search, seizure and forfeiture. It extends such powers, already contained in POCA, to a wider range of assets worth at least a "minimum value" of £1,000 (including valuable personal chattels such as watches, precious stones and artwork). The power is available where there are reasonable grounds to suspect that the assets represent the proceeds of crime or are intended for use in a criminal enterprise.

Furthermore, the CFA provides that forfeiture notices may be made in respect of accounts subject to Account Freezing Orders. The effect of this is that forfeiture powers will be extended to cash in bank accounts where there are reasonable grounds to suspect that the funds are implicated in criminality, but there has not been any charge or conviction.

3.3.4 Super-SARs

Super-SARs are SARs that are effectively the product of information sharing between financial firms such as banks. Until now there were legal limits on the ability of firms to share information about money laundering suspicions. The disclosure of information to a third party where there are suspicions of money laundering could constitute tipping off. To improve the quality of SARs and provide protection to reporters, the CFA allows relevant undertakings to share information about their suspicions. The disclosure of information could be made at the request of the NCA or on the initiative of the firm, but subject to the notification of and approval from the NCA.

There is a degree of scepticism about the extent to which banks may be encouraged to share more information as a result of this measure, especially given the procedures to be followed. Against this background, the authorities consider it to be a significant move forward to enhancing the quality of intelligence available to them and the business sector.

3.3.5 Better SARs

In a separate but related development on SARs, September 2016 saw the publication by the NCA of new guidance to help businesses submit better quality suspicious activity reports.[21] The NCA was concerned that many reports by firms are insufficiently clear and concise, and fail to provide an explicit rationale for suspicion or set out the context of the transaction.

The NCA's guidance emphasises that as suspicion (or reasonable grounds to suspect) is the rationale for submitting a SAR, the grounds for suspicion must be stated explicitly in any report. For example, the SAR should try to explain how the circumstances arose and why the reporter is suspicious. To combat poor-quality reporting, the NCA will in future consider closing its file and requiring a firm to re-submit.

Moreover, the NCA may refer SARs that do not meet its criteria to the AML supervisor for the relevant sector in the case of a regulated entity.

The guidance reminds reporters that the NCA is not a crime reporting agency; when reporting any criminal offence this should be made separately to the appropriate authorities (although the crime reference and organisation details should be included in the SAR). Nor is it the NCA's role to provide advice on whether to make a report. The guidance is clear that reporters must satisfy themselves as to whether they need to make a report. If any advice is required, this should be sought from professional advisers.

The regulated sector is diverse, with some 27 different supervisors, but financial services firms will be anxious to avoid attracting the FCA's attention. The FCA expects its firms to have clear procedures for the reporting of suspicions and for MLROs to investigate appropriately, including instances where few notifications are being made, and investigating the reasons for this. This was something which the MLRO of Sonali Bank was found to have failed to do (see below). In this respect, the FCA expects to see a proper assessment by the MLRO rather than a pure passing on of suspicion reports to the NCA. The FCA highlights in its Financial Crime Guide the importance of SARs being accurate and clear, and in plain English, with cross-references to related SARs where relevant. Decisions about whether or not to report to the NCA should be documented in accordance with a clear process.

4 Sanctions

Compliance with trade and financial sanctions should be high on the radar of all financial institutions given the critical role that these measures play in protecting and promoting the fundamental interests of society. The election of Donald Trump as US President may result in changes to policies on financial sanctions. We will need to wait for developments in this regard. There has also been a significant rise in enforcement actions for violations of trade restrictions. For example, in the UK, there have already been prison sentences, director disqualifications and criminal and administrative fines following violations.

Where a financial institution is found to have breached these controls, its defence will, in relation to a number of the offences, be limited to arguing that it did not know and had no reason to suspect that the financing or financial assistance it was providing would give rise to a breach of the relevant EU sanctions, as enforced by the UK. The burden of proof in establishing this defence will rest with the financial institution. As such, it is vital that financial institutions have clear due diligence protocols that are tailored to address the risks that arise from transactions relating to sanctioned countries and that all stages of the due diligence process are properly documented. Without such documentation, it will be difficult to establish that the financial institution had no reason to suspect its actions amounted to a breach of the applicable sanctions regime.

While there has been limited information released into the public domain to date regarding enforcement action in relation to these controls, the potential penalties are severe, with non-compliant companies being exposed to unlimited fines and individuals potentially facing unlimited fines and/or imprisonment for a maximum of seven years (depending on the severity of the offence).

4.1 Policing and Crime Act 2017

In the UK, the Policing and Crime Act 2017 received Royal Assent on 31 January 2017 and gives HM Treasury (through the OFSI) the power to impose civil penalties for breaches of financial sanctions. This is part of a broader reform of powers to take action in cases of financial sanctions breaches. The Act creates the power to enter into a DPA in respect of a financial sanctions breach. It also creates the power to make a Serious Crime Prevention Order which imposes conditions or restrictions as appropriate to protect the public by preventing or disrupting the future involvement of a person in serious crime.

Financial sanctions commonly used in support of foreign policy include "targeted asset freezes" which seek to restrict the use of funds and economic resources of named individuals or entities, restrictions on financial markets and services (e.g. a requirement to end banking relationships), and directions to end all business of a specified type with an individual, sector or country. While there must be a connection to the UK or UK nexus, a breach of sanctions does not have to take place within the UK for the OFSI to have jurisdiction. In this respect, the Act has not altered the extent of the regime.

Of course, a breach of financial sanctions is a criminal offence punishable with a term of imprisonment. The Act harmonises the maximum penalty for an offence at seven years on conviction (six months on summary conviction) across all financial sanctions regimes. Criminal proceedings are time consuming and costly, and this limits the number of prosecutions that can be brought. As opposed to trade sanctions, there is no ability to impose compound penalties in cases where it is not in the public interest to prosecute. By giving OFSI the power to impose civil fines, the government has expanded the range of tools available to it to address breaches.

A fine can be imposed where HM Treasury is satisfied on the lower civil burden of proof (the balance of probabilities), that there has been a financial sanctions breach and that the offender knew or had reasonable cause to suspect this. HM Treasury must take into account representations from the alleged offender. If it decides to impose a penalty, the offender can ask for this to be reviewed by a government Minister. Thereafter, if still unsatisfied, the matter can be referred to the Upper Tribunal. The system has therefore been set up to make it relatively straightforward to impose a penalty and to minimise judicial involvement.

Where the breach or failure concerns specific funds or economic resources, the maximum level of the penalty is the greater of £1 million or, if higher, 50% of the estimated value. In other cases, the maximum is £1 million. The monetary penalty can be imposed both on a legal entity and also on individuals such as officers of the company who have consented to or connived in the breach or where the breach occurs because of their neglect. The OSFI retains the flexibility to impose a civil penalty on one person in a case and to prosecute another criminally.

The options available to OFSI for a breach of financial sanctions now include:

- requiring details of how a party proposes to improve their compliance practices;
- where there are regulated professionals or bodies referring them to their own professional body to improve their compliance;
- imposing a monetary penalty; and
- a referral to law enforcement agencies for investigation and prosecution as a criminal offence.

In April 2017, after consultation, HM Treasury published guidance over the use of the power to impose civil fines.[22] This sets out the types of conduct and behaviour in relation to which the OFSI will have regard when exercising its power to impose fines. These include:

- the direct provision of funds or economic resources to a designated (sanctioned) person;
- circumvention;
- severity—a high-value breach is more likely to bring enforcement action;
- the harm, or the risk of harm, to the sanction regime's objectives;
- knowledge and compliance in the sector—the failure of regulated professionals to meet any professional standards may be an aggravating factor;
- behaviour (i.e. whether deliberate, by neglect, a failure to take reasonable care, a systems and control failure, an incorrect legal interpretation or if there has simply been a mistake);
- failure to apply for a licence or non-compliance with the terms of a licence;
- professional facilitation (i.e. individuals who act on behalf of or provide advice to others);
- repeated extended or persistent breaches;
- self-reporting breaches to OFSI; and
- public interest, strategic priority and future compliance effect.

The relevant parts of the Policing and Crime Act on sanctions came into force on 1 April 2017.

4.2 Imposing sanctions after Brexit

With the two-year art.50 notice period now counting down to Brexit, HM Treasury and the Foreign Office are consulting on the UK's future legal framework for imposing and implementing sanctions.[23] The consultation seeks views on the legal powers that the government will need post-Brexit to be able to continue to impose sanctions to comply with its obligations under the United Nations Charter. At present reliance is generally placed on the European Communities Act 1972 and it thought that the Great Repeal Bill will not provide the necessary powers. Moreover, the United Nations Act 1946 cannot be used to apply asset freezes since a Supreme Court decision in 2010 which held that the power as exercised under the 1946 Act was not compatible with art.6 of the European Convention on Human Rights.[24]

The new powers need to be similar to those which will be lost. The government intends to maintain its ability to impose travel bans, asset freezes, as well as financial and trade restrictions. The government is proposing to create a legislative framework through primary legislation and to use secondary legislation to quickly implement targeted sanctions. The consultation envisages the ability to impose detailed and comprehensive measures particularly in the financial sector (e.g. investment bans and restricting access to capital markets). In line with recent UK and EU court decisions there will be a power to designate persons (thereby imposing restrictions), where there is sufficient evidence to have "reasonable grounds to suspect" that they meet established criteria.[25] It is also suggested that the government should have power to impose sanctions in support of counter terrorist activity which may entail updating the Terrorist Asset-Freezing etc Act 2010.

The consultation envisages that the new legislation will provide for the review of non-UN sanction regimes from time to time, allow for administrative reviews of sanctions when requested by affected persons and the right of challenge before the courts. As regards the latter, although the government says that it will always seek to rely on "open-source" material when exercising its powers, it intends to put procedures in place to protect sensitive materials from disclosure (closed procedure materials) and make use of special advocates along the lines of the Counter-Terrorism Act 2008. As is currently the case, the proposal will restrict the ability to claim damages against an individual or firm simply due to their compliance with sanctions.

Preserving existing law, it is intended that the legislation would include a duty to report should a person know of, or suspect a breach of financial sanctions. This is intended to promote compliance and provide intelligence. The government promises that the burden on business will be proportionate and no more than is necessary. The consultation also sets out proposals to maintain the current licensing regime and will seek to ensure clarity over these powers. The Export Control Joint Unit will license goods, technology and services as it does now.

The enforcement powers as strengthened by the Policing and Crime Act 2017, discussed above, will be preserved subject to any necessary adjustments to align with the new regime. It is proposed that there will be a power to allow law enforcement to seize property or money from a sanctioned person with a view to freezing those assets.

With regard to AML and CTF legislation generally, the government proposes to use this legislation to enable it post-Brexit (with the repeal of the European Communities Act 1972) to amend and update the regime as a whole and, in particular, the money laundering regulations, when required, in line with FATF recommendations and standards.

5 FinTech and RegTech issues

5.1 5MLD

The use of technology presents its own risks. The terror attacks in Paris and Belgium in 2015/2016 are said to have been funded through the use of pre-paid payment cards. The attraction of these cards, of course, is that they can be subject to lower customer due diligence standards. The Second Payment Services Directive (PSD2)[26] will act as a catalyst for the growth of the FinTech industry, so the sector will need to address the financial crime challenges of new innovative payment products.

5.1.1 Payments and due diligence

The 4MLD and 5MLD both address the risks posed by technology. As discussed already, Annex III to the 4MLD sets out criteria to which firms must have regard in determining whether EDD should be applied in particular circumstances. The list includes products or transactions that might favour anonymity, as well as new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

The 5MLD legislative proposal would make more detailed provision in relation to pre-paid cards. In particular:

- Virtual currencies would be brought within the scope of AML regulation. Virtual currency exchanges, which permit virtual currencies (e.g. Bitcoin) to be converted into fiat currencies (e.g. Sterling or Euro) will be obliged entities under the 4MLD and therefore subject to AML compliance obligations. Custodian Wallet providers, that is providers of services which enable you to hold virtual currencies, would similarly be subject to regulation as obliged entities.
- The scope of the exemption from performing customer due diligence in relation to pre-paid cards would be narrowed—a card purse value of up to €250 would be reduced to €150.
- It would no longer be possible to carry out online transactions with a value of more than €50 on an anonymous basis.
- Card schemes would be under an obligation to prohibit the use of pre-paid cards issued in a jurisdiction that does not have equivalent customer due diligence standards to the EU. As a practical matter this may not be straightforward for schemes to implement.

FinTech companies embracing new technologies, in particular virtual currency operators and wallet providers, may find their business models impeded by these requirements, although regulation might serve to improve their credibility with the public.

5.1.2 Centralised automated mechanisms

Radically, and of potential concern with respect to data protection and the right to privacy, 5MLD requires Member States to establish "centralised automated mechanisms" to quickly identify the natural and legal holders of bank and payment accounts. This obligation again originates from recent terrorist attacks and the perceived need to trace accounts and individuals rapidly.

The proposed legislation gives a choice to Member States between a central registry or central electronic data retrieval systems that FIUs and other authorities can access. Currently, the UK's FIU accesses information on accounts through credit reference agencies and via established contacts with account providers. The UK government has concerns over this proposal on the basis that current arrangements work well. As a result, the UK favours the retrieval system as it is less onerous to implement and avoids the dangers of holding a large quantity of valuable information in one place.

5.2 Cybercrime and financial services firms

FCA Chairman, John Griffith-Jones, in his foreword to the FCA's business plan for 2017/18 states that: "of the increasing risk areas that we have identified, one in particular stands out—cyber resilience. Cyber-attacks are increasing in number, scale and sophistication." There has been a significant increase in attacks reported by firms over the past three years. Cyber-crime is a major theme in this year's business plan and this is reflected in the FCA's cross-sector priorities where, in the context of technological change and resilience, reference is made to the FCA performing technology and cyber-capability assessments on all firms considered "high impact". The growth in the use of technology (e.g. electronic and digital services), including outsourced functions, is said to heighten cyber security risks, provide opportunities for money laundering and increase the likelihood of fraud. Legacy systems (e.g. in banks) are seen as being especially vulnerable to disruption and cyber-attacks.

The UK's conduct regulator is concerned that given their extent, these attacks could affect firms' cyber-resilience and financial crime controls. The FCA calls on firms to improve their capacity to defend and respond to and consider their resilience to, the risk of attack, when developing IT systems and processes. In this regard, the FCA will be working closely with the National Cyber Security Centre and the NCA.

High-impact firms can expect the FCA to carry out technology and cyber capability assessments over this coming year. Beyond that, the regulator wants to see better reporting by the firms it regulates of "resilience incidents" and cyber-attacks and to see better results from the risk assessments that it carries out on firms.

Emphasising the importance placed by the authorities on cyber-security, it was the subject of a recent speech by Nausicaa Delfas, FCA executive director, to the Financial Information Security Network.[27] In a speech which made reference to "some institutions having bitcoin accounts to pay ransoms" a number of steps were flagged up to address the risk posed by cyber attacks. These are:

- getting the basics right: vulnerabilities, many of which firms are aware of, account for 85% of successful breaches;
- moving to a secure culture: rather than relying only on a policy document, staff need to understand the risk and be empowered to act;
- measuring that culture by setting key performance indicators and success criteria besides ensuring that non-executive directors are satisfied that their firm is properly managing cyber risk;
- using other drivers beyond the boardroom, such as institutional investors putting questions to company boards;
- sharing information: the FCA have established Cyber Coordination Groups ("CCGs"), to achieve a better collective cyber capability. The FCA is collecting, anonymising and aggregating risk data from 175 firms across the financial sector to obtain a better picture about how cyber risk crystallises; and
- building capability, under which the UK's National Cyber Security Strategy seeks to tackle the cyber skills shortage and where the FCA supports the UK government's plan to develop a cyber security profession.

6 FCA financial crime initiatives

6.1 Financial crime checklist

On 21 November 2016, the FCA issued a booklet aimed at consumer credit firms setting out good and bad practice on compliance with obligations under the Money Laundering Regulations 2007. While directed at consumer credit firms, the booklet is relevant to all firms subject to the money laundering regime.

Financial crime is one of the cross-sector regulatory priorities for the FCA according to its 2017/18 Business Plan. It continues to be an area of enforcement focus for the FCA. The risks posed to consumer credit firms differ from risks for other financial services firms. According to the Joint Money Laundering Steering Committee, in the consumer finance context the main money laundering risk arises from an acceleration in the repayment schedule, whereby the borrower may seek to use tainted funds to repay borrowings and launder money in that way. Lenders also have to deal with fraud and identity theft issues which can also feed into money laundering concerns.

Of all the issues dealt with, there are two in respect of which firms should place special emphasis.

6.1.1 Governance

The accountability of senior managers to guard against financial crime is provided for under high-level standards in the FCA Handbook in respect of systems and controls. In this regard, a firm must allocate overall responsibility to a director or senior manager (e.g. the money laundering reporting officer). It is vital that proper reporting lines are in place and that information can reach management and relevant committees in a timely fashion for consideration and action, where necessary. With the roll-out of the Senior Managers and Certified Persons Regime to all financial services firms in 2018, the incentive on managers to ensure that reasonable steps have been taken will increase.

6.1.2 Data security

As discussed above, there is also the threat posed by cyber attacks and the corresponding need to ensure data security. The growing use of technology in delivering services to clients, the sheer amount of data

and its nature makes cyber security a key issue. The Data Protection Act 1998 requires that information must be kept securely and protected against criminals who would, for instance, commit identity theft. Good data security policies and appropriate systems and controls are a necessity in ensuring that staff understand their responsibilities and in demonstrating compliance to regulators, including the Information Commissioner's Office with their growing penalty powers. With the coming into force of the EU General Data Protection Regulation and with enhanced sanctions such as significantly higher fines, this is an area where firms will wish to invest. The authorities will be able to fine at least €20 million or 4% of a firm's global annual turnover, whichever is highest.

6.2 Financial Crime Annual Data Return

The FCA has introduced the annual Financial Crime Annual Data Return ("REP-CRIM"), the details of which were set out in its Policy Statement PS16/19 of July 2016. The return requires authorised firms to provide information to the FCA across a range of areas of their business and operations such as the location of customers and the resources allocated to reducing the risk of financial crime. The data will be used to support the FCA's financial crime supervision strategy, helping them to identify financial crime risks and trends, as well as potential emerging issues.

The return is to be completed by firms subject to the Money Laundering Regulations (subject to exceptions for smaller firms) via the FCA's GABRIEL reporting system. Firms must complete and submit the form within 60 business days of their accounting reference date from 31 December 2016. Unhelpfully, many of the questions are ambiguous as to what precise information is sought. This means that it is important for firms to consider how they are going to interpret and respond, and to record the basis for doing so, not least so as to be consistent the next year, but in the worst case, should the FCA ask for an explanation. Given the likelihood of different approaches by firms to completing answers, the value of the information provided is likely to suffer.

7 Case law update: Financial crime cases from 2016/2017

The flow of litigation continues in financial services including both criminal prosecutions and regulatory enforcement. The Serious Fraud Office ("SFO") has enjoyed success with DPAs, most recently with Rolls Royce Plc which concluded a four-year investigation into bribery and corruption. No doubt we can expect to see the tool being used more regularly, and potentially for breaches of financial sanctions in the light of the Policing and Crime Act 2017, as well as corporate liability (if this is reformed) for economic crimes. On the other side of the balance sheet, the SFO's success with Tom Hayes, who was convicted for the manipulation of the LIBOR benchmark, has not continued, with several defendants having been acquitted of late.

The FCA, for its part, has imposed significant financial penalties on Deutsche Bank AG for breach of its high-level principles and Senior Management Arrangements, Systems and Controls ("SYSC"). It found that the bank's AML control framework was substantially inadequate and that certain "mirror" trading conducted in Moscow and London was highly suggestive of financial crime.[29] The case of Sonali Bank on money laundering controls is discussed below.

7.1 Summaries

7.1.1 *R (on the application of Merida Oil Traders Ltd) v Central Criminal Court*, Queen's Bench Division (Administrative Court)

These proceedings concerned the misuse of powers under the POCA and procedural failings. In April 2017, the Administrative Court considered the powers available to law enforcement agencies, such as the police, under POCA, specifically relating to the making of production orders under s.345. Two financial trading companies were under investigation for money laundering offences. Those companies traded through a broker, which terminated their relationship at the outset of the investigation. The police prevented the broker from repaying the companies the closing balances on their accounts on the basis that they intended to confiscate those funds under POCA. The police asked the broker to write cheques to the companies which would be susceptible to production orders made under POCA. The broker complied, and the police made applications to court without notice, which were granted the same day, with an

application notice for a detention order following shortly afterwards. The proceedings in fact took place in a different court to the one originally notified to the companies, and the original notification of the application was received by only one company.

The companies applied for a judicial review of the exercise of these powers under the POCA. The Court found that:

- the statutory requirements for making the production orders had not been met—there were no reasonable grounds for believing that the cheques were "likely to be of substantial value to the investigation for the purposes of which the order was sought";
- the cheques had not been lawfully seized, as the police had engineered and adopted an unlawful procedure whereby the closing balances were converted into cash at the instigation of the police for the purpose of subjecting the balances to this process;
- the production orders were not sought for a lawful purpose;
- the detention orders were not lawful, as the cash had not been lawfully seized, for the above reasons; and
- there had been procedural impropriety, as the police had breached their duty of disclosure by failing to give the companies sufficient notice of their application for a production order.

The Court maintained that only in exceptional circumstances could it depart from the principle that orders should not be made which affected a person's rights without first giving them an opportunity to be heard. The reasons relied upon by the police were "untenable". The Court ordered the police to release the companies' funds, and it granted a declaration that s.294 of POCA could not be used to seize the cheques.

7.1.2 *National Crime Agency v N* [2017] EWCA Civ 253, in relation to *N v S* [2015] EWHC 3248 (Comm)

In April 2017, the Court of Appeal granted an appeal by the National Crime Agency ("NCA") confirming the courts' reluctance to oust a moratorium under the money laundering consent regime.

At first instance, the court considered an application for an injunction by the bank's customer to force the bank to carry out transactions on the customer's accounts. The bank had previously filed a suspicious activity report with the NCA to the effect that it suspected the customer's accounts contained the proceeds of investment fraud and had frozen the accounts accordingly. The NCA was an interested party in the proceedings at first instance.

The court found in favour of the customer and granted an injunction stating that the bank would not commit a criminal offence under POCA for operating the accounts. This effectively ousted the POCA consent regime and constituted a different approach to most recent case authorities, where the courts have generally refused to interfere with the POCA consent regime. The NCA appealed the judgment.

On appeal, the Court of Appeal found that, while ordinarily the court should not intervene with the seven-day notice and 31-day moratorium periods under POCA, there is jurisdiction to grant interim relief in appropriate cases. The Court of Appeal noted, regarding the declaration of no criminal liability made by the court at first instance, that such a declaration should be made only when the court has sufficient assurance as to the recipients' entitlement. In this case it found that the court did not have that assurance as there had not been a thorough consideration of the bank's suspicions that there was criminal property in the customer's accounts.

The Court of Appeal's decision confirms that while bank customers may seek injunctions from the courts where their assets have been frozen, the courts will not readily intervene to override the consent regime.

7.1.3 FCA Final Notice: Tesco Stores/Tesco Plc, 28 March 2017

The FCA took action for market manipulation against Tesco arising out of erroneous statements made to the market. On 28 March 2017, the FCA published a Final Notice finding that Tesco Plc and Tesco Stores Ltd (together "Tesco") had committed market abuse in relation to a trading statement made in August 2014 which overstated its expected profit. The FCA required Tesco to pay restitution to those investors who had suffered a loss as a result of the creation of a false market and for the overpayment of Tesco's securities in 2014.

Tesco Plc had published a trading statement in August 2014 (the "August Statement"), which updated the market on Tesco Plc's expected trading profit for H1 2014/2015 and expected trading profits for the full year 2014/2015. In preparing the August Statement, the Tesco Plc Board relied on accounting information provided to it by Tesco Stores Ltd which was incorrect and which did not disclose the fact or risk of an inaccuracy in its profits. Those staff who were aware of the actual position failed to alert the Tesco Plc Board about the inaccuracy. Subsequent to publishing the August Statement, Tesco Plc made a number of related announcements, admitting that it had overstated the H1 2014/2015 profit by £76 million and that the total overstatement of actual and expected profit was £284 million.

The FCA has required Tesco to pay restitution to investors who purchased Tesco shares and bonds on or after the date of the Autumn Statement and who still held those securities when the statement was corrected in September 2014. It estimated that the total amount of compensation that may be payable is approximately £85 million, plus interest. This is the first time that the FCA has used its powers under s.384 of the Financial Services and Markets Act 2000 to require a listed company to pay compensation for market abuse.

The FCA found that:

- Tesco knew, or could reasonably have been expected to have known, that the information in the August Statement was false or misleading;
- there was knowledge at a sufficiently high level (but below the level of the Tesco Plc Board) as to the false and misleading nature of the August Statement for that knowledge to constitute the knowledge of Tesco Plc, within the specific context of, and for the purposes of, market abuse;
- the provision by Tesco Stores Ltd of incorrect information to Tesco Plc amounted to dissemination of it and Tesco had therefore engaged in market abuse contrary to s.118(7) of the Financial Services and Markets Act 2000 (as it was then in force);
- as a result of this market abuse, a false market was created in the relevant securities and purchasers of such securities paid a higher price than they would have paid had there not been a false market; and
- the false market substantially came to an end when Tesco corrected the August statement in September.

The FCA stressed that it was not suggesting that the Tesco Plc Board knew, or could reasonably be expected to have known, that the information in the August Statement was false or misleading.

There are a number of lessons that listed companies can learn from these events, the key ones being:

- It is critical to have an effective set of systems and controls in place which operate across a company's group, and not just at the public limited company level. This is particularly the case for monitoring and disclosing inside information and financial information. Such systems and controls should be kept under regular review and there should be frequent training on them for relevant personnel.
- It is important for a company's operations to embrace a culture of openness and transparency, and this should be regarded as at least as important as financial performance.
- In the event that there is a potential breach of the rules, it is critical to rectify this promptly. In the immediate term, this might involve publishing a correcting announcement to the market as soon as possible, but will also involve dealing with the regulators in an open and co-operative manner and taking steps to prevent future breaches of the rules.

7.1.4 *Property Alliance Group Ltd v Royal Bank of Scotland Plc* [2016] EWHC 3342 (Ch)

In December 2016, the High Court dismissed all claims in this interest rate swaps mis-selling and LIBOR manipulation case. The claim arose out commercial banking services provided by Royal Bank of Scotland ("RBS") to Property Alliance Group ("PAG").

PAG claimed that RBS had mis-sold them the swaps as they did not provide a solution to, or protect them from, exposure to interest rate risk, and so they could not be said to have provided the intended interest rate hedge as they had, in fact, left PAG in a worse position.

This case marks the first civil decision at trial relating to allegations around LIBOR manipulation. Mrs Justice Asplin, sitting in the Chancery Division's Financial List, rejected claims that there were implied representations or implied terms as to LIBOR made by RBS that had induced PAG to enter into the various swap agreements. Similarly, PAG's claims for rescission and damages as a result of alleged misrepresentation, misstatement and breach of implied terms were dismissed.

In reaching her conclusions, the judge considered a number of leading cases, including *Marks and Spencer Plc v BNP Paribas Securities Services Trust Company (Jersey) Ltd* [2015] UKSC 72 (concerning implied terms), and *IFE Fund SA v Goldman Sachs International* [2007] EWCA Civ 811 (concerning implied representations). These proceedings follow three other key *PAG v RBS* cases from 2015 that concerned issues of confidentiality and disclosure, without prejudice communications, and legal privilege. [30]

7.1.5 FCA Final Notice Tariq Carrimjee, 22 November 2016/*Carrimjee v FCA* [2016] UKUT 0447 (TCC)

Mr Carrimjee was an experienced investment adviser and partner in a wealth management business. He was approved by the FCA to perform various significant influence and controlled functions including: chief executive (CF3), partner (CF4), compliance oversight (CF10) and money laundering reporting (CF11). He failed to spot the warning signs around market abuse and act appropriately.

The FCA found that Mr Carrimjee had failed to act with integrity in breach of the Statements of Principle for Approved Persons when he recklessly assisted a client to manipulate the closing price of global depositary receipts in two companies in April and October 2010. In this respect, the FCA considered that he suspected that his client intended to commit market manipulation, yet turned a blind eye to that risk and recklessly assisted his client in the attempt. He had either failed to appropriately identify the risk of market abuse or had done nothing to address his concerns besides seeking inadequate reassurances from a colleague.

In November 2016, the FCA issued a Final Notice to Tariq Carrimjee, prohibiting him from performing the compliance and money laundering reporting significant influence functions in relation to any regulated financial activity. Mr Carrimjee was also subject to a financial penalty of £89,004. This Notice was followed by reference to the Tribunal which, in its judgment, concluded that the FCA's action was appropriate on the facts, although on the basis that Mr Carrimjee had failed to act with due skill, care and diligence, rather than a lack of integrity, as the FCA had originally contended.

Mr Carrimjee argued that the failings represented "a one-off incident which occurred nearly six-and-a-half years ago whereas there [was] a wealth of evidence since that time to support his competence to perform the relevant functions". The Tribunal, however, concluded that the misconduct "arose out of dealings and discussions which took place over a number of days during which Mr Carrimjee had adequate time to reflect and consider whether his concerns should be escalated". They could not, therefore, be described as a "momentary lapse of judgment".

A number of legal issues arose in the course of the Tribunal's decision, including confirmation that the civil standard of proof applies to all disciplinary (e.g. the imposition of financial penalties for breach of the Statements of Principle) and non-disciplinary references (where a prohibition is imposed to protect the market).

7.1.6 FCA Final Notice Sonali Bank (UK) Ltd, 12 October 2016

In October 2016, the FCA published a Final Notice imposing a fine of £3.25 million (after an early settlement discount) on Sonali Bank (UK) Ltd ("Sonali Bank"). In a separate Final Notice, a fine of £17,900 was imposed on Sonali Bank's MLRO. As a further disciplinary measure, Sonali Bank was also prevented from accepting deposits from new customers for 168 days.

Sonali Bank is the UK subsidiary of Sonali Bank Ltd, which is based in Bangladesh. The former's activities include the international transfer of funds, the remittance of cash and other non face-to-face business, each posing significant AML risks. In this regard, Bangladesh is regarded as a higher risk jurisdiction. The FATF Mutual Evaluation Report of July 2009 states that Bangladesh "faces significant risks of money laundering and some risks of terrorism financing".

With respect to Sonali Bank, the FCA found that there was a "surprising" lack of SARs made by the bank's staff, particularly in relation to its trade finance business. Despite recognising this fact, the bank's MLRO failed for three successive years to establish the reasons for the absence of SARs. A Skilled Person's Report found that there was a systemic failure to carry out sufficient customer due diligence. This manifested itself in scanned documentation that was unclear, out-of-date identification, incomplete account opening forms and insufficient information about expected account activity.

The FCA found that Sonali Bank had failed to take reasonable care to manage its AML risks, breaching Principle 3 of the Principles for Businesses, and that it had breached Principle 11 by failing to notify the FCA for at least seven weeks about a potentially significant fraud with respect to one of its customer's accounts. The Final Notice contains a long list of failings, ranging from a failure to ingrain compliance throughout the business, to seeing that senior management were provided with sufficiently clear information, to ensuring that the MLRO was adequately resourced. In short, there were serious and systemic weaknesses in relation to AML governance and control systems which extended to all levels of the business and governance structure, including the senior management team, the MLRO function, oversight of UK branches, and policies and procedures in relation to AML.

The Final Notice issued to the MLRO notes that Sonali Bank had failed to put in place compliance monitoring measures which were appropriately focused on the specific risks relevant to the business, despite the warnings of internal auditors and the fact that the MLRO knew that the FCA had identified serious failings in the bank's systems and controls. The FCA noted that the MLRO suffered from a lack of resource in the MLRO department, but considered that he had failed to adequately raise the issue with senior management. In particular, the FCA noted that the MLRO failed to put in place effective systems and controls for ensuring that staff were aware of their AML responsibilities and complied with them. Rather, he continued to reassure the board and other senior management that staff adequately understood their obligations.

The FCA's Final Notices show a business where there were serious and widespread failings. Compliance officers should take note that they cannot seek refuge in these failings, nor cite a lack of resources to meet their obligations.

7.1.7 *SFO v ENRC* [2017] EWHC 1017 (QB), 9 May 2017

On 9 May 2017, the High Court gave judgment in favour of the SFO, finding that certain categories of documents produced by Eurasian Natural Resources Corporation Ltd ("ENRC") during an internal investigation were not covered by litigation privilege.

It may be more difficult in future for companies to claim litigation privilege over documents produced as part of their internal investigations, even after a criminal investigation has been commenced or the SFO has sought to exercise its powers under Section 2. In order to rely on litigation privilege with respect to those documents, the company in question will need to show that, at the time of the internal investigation, it genuinely considered that a criminal prosecution was reasonably contemplated.

In 2011, ENRC began an internal investigation following whistle-blower allegations of fraud, bribery and corruption in Kazakhstan and an African country. ENRC began communicating regularly with the SFO from August 2011, which led to the SFO launching its own criminal investigation in April 2013.

As part of its investigation, the SFO exercised its powers under s.2(3) of the Criminal Justice Act 1987, compelling ENRC to produce documents relevant to the investigation. The SFO's powers of compulsion do not extend to documents that are subject to litigation privilege, which ENRC claimed applied to certain categories of "disputed documents".

Litigation privilege applies to communications made between parties, or their solicitors and third parties, for the sole or dominant purpose of conducting existing or contemplated adversarial litigation. The Court, therefore, had to determine the extent to which litigation privilege applied to the disputed documents.

The Court held that litigation privilege did not apply to the disputed documents, as ENRC could not demonstrate that adversarial litigation was contemplated at the time that they were produced. The Court cited *United States v Phillip Morris Inc* (No.1) [2003] EWHC 3028 (Comm) in its decision stating that for litigation privilege to apply, it was for ENRC to establish that, as of the date it approached the SFO, it was

"aware of circumstances which rendered litigation between itself and the SFO a real likelihood rather than a mere possibility".

The Judge's reasoning was that a criminal investigation does not necessarily mean that a prosecution is reasonably in contemplation and she did not consider that a criminal investigation was sufficiently adversarial for litigation privilege to apply. This decision therefore casts doubt over the ability to rely on litigation privilege, even after a criminal investigation has been commenced or a Section 2 Notice has been issued (which allows the SFO to search premises or compel the production of documents or information).

An appeal from this decision is likely. In the meantime, however, companies will need to consider carefully, at the outset of any investigation, whether and at what stage privilege is applicable, including whether a prosecution is reasonably in contemplation.

Notes

1. SI 2015/878.
2. Home Office and HM Treasury, Action Plan for Anti-Money Laundering and Counter-Terrorist Finance, April 2016. See *https://www.gov.uk/government/publications/action-plan-for-anti-money-laundering-and-counter-terrorist-finance* [Accessed 18 May 2017].
3. FCA, Business Plan 2017/18, April 2017. See *https://www.fca.org.uk/publication/business-plans/business-plan-2017-18.pdf* [Accessed 18 May 2017].
4. FCA Final Notices to Niall O'Kelly and Lukhvir Thind, 7 April 2017.
5. HM Treasury, Consultation on the Transposition of the Fourth Money Laundering Directive, September 2016. See *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/553409/4mld_final_15_sept_2016.pdf* [Accessed 18 May 2017] and Response *https://www.gov.uk/government/consultations/money-laundering-regulations-2017/money-laundering-regulations-2017* [Accessed 18 May 2017].
6. European Parliament, Working Document on the Inquiry into Money Laundering, Tax Avoidance and Tax Evasion, 15 December 2016. See *http://www.europarl.europa.eu* [Accessed 18 May 2017].
7. Commission Delegated Regulation 2016/1675 Supplementing Directive 2015/849 by Identifying High-risk Third Countries with Strategic Deficiencies.
8. Joint Committee of ESAs, Joint Guidelines under arts 17 and 18(4) of Directive 2015/849 on Simplified and Enhanced Customer Due Diligence, JC 2015 061, 21 October 2016.
9. HM Treasury & Home Office, UK National Risk Assessment of Money Laundering and Terrorist Financing, October 2015. See *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf* [Accessed 18 May 2017].
10. The Law Society Response, HM Treasury Consultation on the Money Laundering Regulations, April 2017.
11. Joint Committee of ESAs, Draft Joint Guidelines under art.25 of Regulation (EU) 2015/847 on the Measures Payment Service Providers Should Take to Detect Missing or Incomplete Information on the Payer or the Payee, and the Procedures They Should Put in Place to Manage a Transfer of Funds Lacking the Required Information, JC/GL/2017/16, 5 April 2017. See *https://www.eba.europa.eu/documents/10180/1807814/Consultation+Paper+on+draft+Joint+Guidelines+to+prevent+transfers+of+funds+can+be+abused+for+ML+and+TF+%28JC-GL-2017-16%29.pdf* [Accessed 18 May 2017].
12. FCA Guidance Consultation, Guidance on the Treatment of Politically Exposed persons under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, March 2017. *See https://www.fca.org.uk/publication/guidance-consultation/gc17-02.pdf* [Accessed 18 May 2017].
13. See *http://www.jmlsg.org.uk/consultations* [Accessed 18 May 2017].
14. HM Treasury, Anti-money Laundering Supervisory Regime: Response to the Consultation and Call for Further Information, March 2017. See *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/600340/Anti-Money-Laundering-Supervisory-Regime-response-call-for-further-information.pdf* [Accessed 18 May 2017].
15. HM Treasury, Money Laundering Regulations 2017: Consultation, 15 March 2017.
16. Department for Business, Energy & Industrial Strategy, Call for Evidence on a Register Showing Who Owns and Controls Overseas Legal Entities that Own UK Property or Participate in UK Government

Procurement, April 2017. See *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/606611/beneficial-ownership-register-call-evidence.pdf* [Accessed 18 May 2017].
17. Home Office and HM Treasury, Action Plan for Anti-Money Laundering and Counter-Terrorist Finance, April 2016. See *https://www.gov.uk/government/publications/action-plan-for-anti-money-laundering-and-counter-terrorist-finance* [Accessed 18 May 2017].
18. HMRC, Tackling Tax Evasion: Draft Government Guidance for the Corporate Offence of Failure to Prevent the Criminal Facilitation of Tax Evasion, October 2016.
19. Ministry of Justice, Call for Evidence on Corporate Liability for Economic Crime, January 2017. See *https://consult.justice.gov.uk/digital-communications/corporate-liability-for-economic-crime/supporting_documents/corporateliabilityforeconomiccrimeconsultationdocument.pdf* [Accessed 18 May 2017].
20. HM Treasury & HM Revenue & Customs, Tackling Tax Evasion and Avoidance, Cm 9047, March 2015. See *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413931/Tax_evasion_FINAL__with_covers_and_right_sig_.pdf* [Accessed 18 May 2017].
21. NCA, Guidance on Submitting Better Quality SARs, September 2016. See *http://www.nationalcrimeagency.gov.uk/publications/732-guidance-on-submitting-better-quality-sars/file* [Accessed 18 May 2017].
22. HM Treasury, Monetary Penalties for Breaches of Financial Sanctions, Guidance, April 2017. See *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/605884/Monetary_penalties_for_breaches_of_financial_sanctions.pdf* [Accessed 18 May 2017].
23. HM Treasury & Foreign Office, UK's Future Legal Framework for Imposing and Implementing Sanctions, Consultation Cm 9408, April 2017. See *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609986/Public_consultation_on_the_UK_s_future_legal_framework_for_imposing_and_implementing_sanctions__Print_pdf_version_.pdf* [Accessed 18 May 2017].
24. *HMT v Ahmed* [2010] UKSC.
25. *Youssef v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKSC.
26. Directive on Payment Services 2015/2366.
27. Nausicaa Delfas, FCA Executive Director, Speech on "Expect the unexpected—cyber security—2017 and beyond," 24 April 2017. See *https://www.fca.org.uk/news/speeches/expect-unexpected-cyber-security-2017-and-beyond* [Accessed 18 May 2017].
28. SFO, Press Release, SFO completes £497.25m Deferred Prosecution Agreement with Rolls-Royce Plc, 17 January 2017. See *https://www.sfo.gov.uk/2017/01/17/sfo-completes-497-25m-deferred-prosecution-agreement-rolls-royce-plc/* [Accessed 18 May 2017].
29. FCA Final Notice to Deutsche Bank AG, 30 January 2017. *See https://www.fca.org.uk/publication/final-notices/deutsche-bank-2017.pdf* [Accessed 18 May 2017].
30. These cases were discussed in Edition 133 of February 2016.

COMPLIANCE OFFICER BULLETIN

Issue 148—FCA and PRA Enforcement Action: Themes and Trends

Authors: Travers Smith Regulatory Investigations Group

For many people, 2016 proved to be a year of unexpected surprises and so it proved in relation to FCA enforcement. At the end of 2015, a number of observers noted that the recent trend of ever-increasing total annual penalties figures published by the FCA's Enforcement Division appeared to have gone into reverse, with a decline to approximately £905 million. Few would have predicted, however, that the level of FCA penalties levied throughout 2016 would undergo a sudden collapse, declining to approximately £22 million (or £35 million if an additional penalty imposed on Shay Reches requiring contributions to certain failed insurers is included). Nonetheless, as is so often the case, the numbers on their own do not tell the whole story.

First, the wave of enormous fines for LIBOR manipulation which contributed a significant proportion of some final annual totals had finished by 2016, although criminal cases against individuals accused of LIBOR-related offences continued throughout the period. Secondly, a number of sizeable firms that were subject to enforcement action during 2016 were insolvent and their clients were, to the extent that they were eligible, claiming compensation from the Financial Services Compensation Scheme. As a result, the FCA had little scope to impose significant financial penalties and would not have wanted to reduce the pool of potentially recoverable funds. Thirdly, many of the subjects of enforcement action in 2016 were individuals who, by their nature, tend to have more limited financial resources than firms and are typically subject to much smaller fines. Since regulatory enforcement action can have a very severe impact on an individual's career within the financial services sector (and potentially beyond), this apparent focus on greater individual accountability should be a sobering prospect, irrespective of the final size of any penalties imposed. Finally, the first few months of 2017 have already seen an increased level of penalties, bolstered primarily by the £163 million fine imposed on Deutsche Bank in relation to financial crime systems and control issues. It is therefore clear that any talk of the death of the era of big penalties may be somewhat premature.

Early 2017 also saw the resolution of the long-running case brought by Achilles Macris, relating to the circumstances in which an individual can be said to have been identified by the FCA in references in a public enforcement notice, such that (s)he should benefit from a right to make representations about any such references. The final position reached by a majority of the UK Supreme Court may have significant implications for individuals in the future and the judgment deserves detailed consideration.

Overall, 2016 and early 2017 still contained the by-now familiar mix of cases relating to inappropriate market conduct, failure to understand and apply money laundering requirements, breaches of the client money rules, and individuals failing to adhere to the required standards of integrity. Clearly, while the level of penalties may fluctuate from year to year, there is a somewhat disappointing consistency in the type of mistakes that give rise to enforcement.

In this issue, members of the Travers Smith Regulatory Investigations Group consider the implications of some of the more important FCA and PRA enforcement actions that were published between 1 March 2016 and 31 May 2017 and the lessons that can be learnt by firms and individuals.

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 14 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.