THE CITY LIBRARY

ISSUE 188 – August 2021

COMPLIANCE OFFICER BULLETIN

Money Laundering and Financial Crime

The authors are all lawyers in Paul Hastings' London Office. They specialise in advising clients on financial services, regulatory issues, and also in dealing with money laundering and other complex financial crime issues. The Paul Hastings team also regularly represents institutions and individuals in regulatory enforcement and criminal investigations.

Arun Srivastava, Partner

Jonathan Pickworth, Partner

Nina Moffatt, Senior Associate

Konstantin Burkov, Associate

Gesa Bukowski, Associate

William Knox, Trainee

1. Introduction

The money laundering framework shows signs of maturing and consolidating in major markets around the world. The EU has recently announced plans to create a new anti-money laundering supervisor as part of its consolidation of anti-money laundering supervision across the EU. The proposed Anti-Money Laundering Authority will be established as a new EU agency which will perform a co-ordinating role across the EU as the block moves towards a single European rulebook. The implementation of the EU's Sixth Money Laundering Directive will harmonise criminal law on money laundering across the EU. Elsewhere, in the US, laws updating the Bank Secrecy Act, including the 2001 USA PATRIOT Act have been enacted and are being implemented. The Anti-Money Laundering Act 2020 makes changes to the AML/CTF framework in the US including implementation of national priorities, consideration of cryptocurrencies as currencies for purposes of AML/CTF, as well as procedures to track beneficial ownership.

CONTENTS

THOMSON REUTERS™

© 2021 Thomson Reuters. Crown copyright material is reproduced with the permission of the Controller of HMSO and the Queen's Printer for Scotland.

All rights reserved. No part of this publication may be reproduced, or transmitted, in any form or by any means, or stored in any retrieval system of any nature without prior written permission, except for permitted fair dealing under the Copyright, Designs and Patents Act 1988, or in accordance with the terms of a licence issued by the Copyright Licensing Agency in respect of photocopying and/or reprographic reproduction. Application for permission for other use of copyright material, including permission to reproduce extracts in other published works, should be made to the publishers. Full acknowledgement of author, publisher and source must be given.

Thomson Reuters, the Thomson Reuters Logo and Sweet and Maxwell® are trademarks of Thomson Reuters. No responsibility can be accepted by the publisher or the contributors for any action taken as a result of information contained within this publication. Professional advice should always be sought for specific situations.

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

ISSN: 1478-1964

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

HOW TO PLACE YOUR ORDER

Online @
http://www.tr.com/uki-legal-contact

By Phone
0345 600 9355 (UK)

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

In the UK money laundering has remained in focus for regulators in the financial services and other sectors, including the art sector which is likely to come under greater scrutiny after HMRC published its first risk assessment on art market participants in June 2021. The UK Gambling Commission, for example, has been active in imposing fines for AML breaches. HMRC has also taken serious enforcement action and in January 2021 imposed a £23.8 million fine on MT Global which is a money service business, for breaches of the Money Laundering Regulations. In a speech given in March 2021, Mark Steward, the FCA's enforcement head noted that in the last 12 months two of the biggest sanctions imposed by the FCA related to failures to address financial crime and AML risks. Both cases highlighted inadequate systems and controls "where one could be forgiven for thinking the true function and meaning of the controls had become lost in elaborate processes leading to failure". Clearly, the FCA is keen for firms to focus on the harm that regulations are seeking to prevent as opposed to treating regulations as an end in themselves.

Another sign that the FCA continues to take AML and CTF breaches seriously is the fact that it currently has around 42 AML investigations ongoing into firms and individuals. The FCA has also announced its first criminal prosecution against a bank for breaches of the Money Laundering Regulations. This delivers on Mark Steward's much heralded dual track approach to AML investigations.

As with many legal and regulatory issues, developments in the AML and CTF compliance world are influenced by developments in the broader economy and society. The last year has seen the dramatic rise in popularity of crypto-currencies and other digital assets. It has also seen a close focus on environmental issues and sustainable investing. Both areas are the focus of change in AML requirements and policy, as evidenced by the outcome of FATF's recent plenary.

The UK has also taken a further step in its review of corporate criminal liability for economic crime. Successive UK Governments have been mulling over the idea of changing the laws on corporate liability for economic crime offences. In 2017 the Ministry of Justice published a Call for Evidence on Corporate Liability for Economic Crime. The evidence submitted to the Call for Evidence was judged by the Government to be inconclusive. In November 2020, the Government asked the Law Commission to examine the issue and publish a paper providing an assessment of different options for reform. In June 2021, the Law Commission published a Discussion Paper on Corporate Criminal Liability which considers how the law relating to corporate criminal liability can be improved to appropriately capture and punish criminal offences committed by corporations, their directors and senior management.

The AML and CTF world therefore remains an active area where appetite for enforcement and ever changing laws and obligations keep the stakes high for firms and individuals alike.

2. Outcomes from FATF June 2021 plenary meeting

Between 21–25 June 2021, the Financial Action Task Force ("FATF") virtually came together for its plenary meeting following which it published a document setting out its outcomes. This was the fourth plenary meeting under the German Presidency of Dr Marcus Pleyer.

Delegates of the FATF finalised work in a number of important areas including a report that details the financial flows linked to environmental crime and a report on the financing of ethnically or racially motivated terrorism, which were both priorities under the FATF's German Presidency. In addition to this, one notable agreement reached was to publish a white paper which sets out public consultation aimed at transparency and beneficial ownership of legal entities in order to try and improve measures aimed at fighting criminal activity and proceeds of crime in this area.

The publication is broken down into two sections. The first sets out the Strategic Initiatives which address broader, multi-jurisdictional mutual aims, and can be separated into nine separate sub-headings which are addressed below. The second section address specific jurisdictions such as the mutual evaluation of Japan and South Africa, which aims to assess each country's efforts of tackling money laundering in their respective jurisdictions.

The main focus of discussion was aimed at improving risk-based supervision to prevent money laundering and terrorist financing, and updating guidance to help nations and financial institutions better investigate and prosecute terrorist financing and illicit arms trafficking, assess and mitigate the risks of the financing of the proliferation of weapons of mass destruction ("WMDs"), and better understand ways to deal with virtual assets and virtual asset service providers under their anti-money laundering and counter-terrorist financing ("AML" and "CFT" respectively) obligations.

2.1 Strategic initiatives

2.1.1 Exploring the opportunities and challenges of digital transformation of AML/CFT

During the German Presidency, the FATF sought to explore the benefits which could be provided by technology in helping transform the AML and CFT efforts globally, where progress on advanced analytics and machine learning in detecting suspicious activities of money laundering and terrorist financing has been sought.

The FATF finalised a report that identifies emerging and available technology-based solutions, which highlights the necessary conditions, policies and practices that need to be in place to successfully use these technologies to improve the efficiency and effectiveness of AML/CFT. The report was published on 1 July, and also examines the obstacles that could stand in the way of successful implementation of the technology. Such new technologies include innovative skills, methods, and processes that are used to achieve goals relating to the effective implementation of AML/CFT requirements or innovative ways to use established technology-based processes to comply with AML/CFT obligations.

Furthermore, the FATF examined new technologies to assist with data protection and privacy, whilst also allowing governments to fight money laundering and terrorist financing. They noted that this is a significant area of public interest and there are potential conflicts between the need to access relevant information and certain aspects of data privacy. The report highlights these specific new challenges but also the opportunities which new technologies present in assisting AML and CFT.

2.1.2 Virtual assets: Adoption of second 12-month review of implementation

The FATF meeting finalised a second review of the implementation of the FATF's revised Standards on virtual assets and Virtual Asset Service Providers ("VASPs"). So far, 58 out of 128 reporting jurisdictions advised that they have implemented the revised FATF Standards, with 52 of these regulating VASPs and six of these prohibiting the operation of VASPs. However, the majority of jurisdictions have failed to implement the FATF recommendations, which they emphasise leaves holes which may allow for jurisdictional arbitrage for the misuse of virtual assets. The meeting also resolved to finalise the FATF revised guidance which will help to assist jurisdictions and the private sector in implementing the revised standards. This revised guidance is due to be finalised in October 2021.

2.1.3 Money laundering from environmental crime

The FATF noted that there has been "limited action by governments and the private sector to identify, investigate and prosecute laundering of proceeds" from crimes such as illegal mining, logging and land clearing which they state have therefore become "low risk, high reward" activities. The FATF finalised a report which highlighted the scale and money laundering techniques of environmental crimes, particularly the mingling of illegal trade goods themselves with legal trade goods early in the supply chain to make detection of illegal activity far more difficult. The report encourages greater collaboration between AML authorities and environmental crime investigators, to better combat this growing area of money laundering.

2.1.4 Ethnically or racially motivated terrorism financing

The FATF finalised a report on what has come to be known as "Extreme Right-Wing Terrorism" ("ERT") from which attacks from various individuals and groups has grown in recent years. The FATF notes that few of these extreme groups have been categorised as terrorists and encourages these groups to be considered in national risk assessments going forward, as such groups become more sophisticated.

2.1.5 Operational challenges associated with asset recovery

The meeting noted that asset recovery is "at the core of the FATF Recommendations", yet most countries only managed to achieve "low or moderate levels of effectiveness in their ability to confiscate the proceeds of crime." The FATF finalised a report for government authorities that analyses the key obstacles to asset recovery and how to overcome them. The FATF will consider how to follow up on this at the October 2021 meeting.

2.1.6 Guidance on proliferation financing risk assessment and mitigation

Guidance has now been prepared to assist public and private sectors in conducting their risk assessments surrounding proliferation financing risks. Proliferation financing is the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons, and the FATF guidance for this aims to provide public and private bodies with the advice to spot such activities.

2.1.7 Strengthening the FATF standards on beneficial ownership: Public consultation

Improving beneficial ownership transparency of companies and other entities is considered by the FATF as a crucial aspect to combatting money laundering and terrorist financing. The FATF again highlighted that many jurisdictions are still failing to keep beneficial ownership information up to date and available to help combat this issue, something they first highlighted in 2003. The FATF is now considering amendments to strengthen Recommendation 24, Transparency and Beneficial Ownership of Legal Arrangements, including addressing areas such as:

- adequate, accurate, and up-to-date information;
- access to information;

- risk-based approach for foreign legal persons;
- multipronged approach to collection of beneficial ownership information; and
- bearer shares and nominee arrangements.

The FATF has announced that a white paper will be published and has invited public consultation from various stakeholders by 27 August 2021. The next steps will then be discussed at the October 2021 meeting.

2.1.8 Mitigating the unintended consequences of the FATF Standards

A project was launched in February to assist with combating "unintended consequences resulting from the incorrect implementation of the FATF Standards." The FATF plans on analysing possible options in mitigating such issues.

2.2 Country-specific processes

2.2.1 Mutual evaluation of South Africa

The meeting agreed that South Africa has a suitable framework for AML issues but noted that "significant shortcomings remain." Amongst a number of recommendations made to South Africa, one of the areas for improvement was the provision of beneficial ownership information as mentioned above.

2.2.2 Mutual evaluation of Japan

It was noted that Japan has been successful of late in "understanding, identifying and assessing" its money laundering and terrorist financing risks but there are still areas for improvement in some areas, such as supervision of and preventative measures by financial institutions and designated non-financial businesses and professions. Both reports on South Africa and Japan will be published in August 2021.

2.2.3 Jurisdictions under increased monitoring

The FATF has updated the list of countries which it has placed under increased monitoring to include countries such as Malta and the Philippines, and has also removed Ghana from its increased monitoring regime.

2.3 Conclusion

The FATF noted increased difficulties in implementing its standards globally in the face of struggles related to Covid-19 which has exacerbated difficulties in implementing recommended measures.

However, the emphasis on areas such as environmental crime and the continued battle for transparency over beneficial ownership of legal persons appear likely to continue for some time to come.

3. FCA Dear CEO Letter: Areas to focus on and improve

On 21 May 2021, the FCA wrote a "Dear CEO Letter" to retail banks setting out common control failings identified in banks' anti-money laundering frameworks. The Dear CEO Letter encourages senior management of banks to carefully consider its contents and take the necessary steps to gain assurance that financial crime systems and controls are commensurate with the bank's risk profile and meet the requirements of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLR"). Firms should perform a gap analysis against the issues identified by the FCA by 17 September 2021 and take reasonable steps to close any gaps identified. The FCA's Dear CEO Letter is based on weaknesses commonly identified during firm-specific assessments.

Issue	Details	Follow-Up
1. Governance and Oversight	**(a) Structure of the Three Lines of Defence Model ("3LOD")** The 3LOD is the bedrock for internal systems and controls frameworks. There can, however, be difficulties in implementing this framework and also understanding respective roles and responsibilities, particularly between the front office, compliance and internal audit. Front office staff will have the best understanding and knowledge of clients so are best placed to perform the first line of defence role. On the other hand, resourcing and structural issues within organisations mean that the front office is often dependent on other functions within the organisation to assist in the discharge of responsibilities. This is particularly so where processes such as customer due diligence and transaction monitoring are automated or rely on electronic verification which is carried on behind the scenes. In relation to this, the FCA's Dear CEO Letter states that firms often blur responsibilities between the first line, business roles, and second line, compliance roles. The FCA goes on to state that it has identified circumstances where compliance departments undertake first line activities, including completing all due diligence checks or all aspects of customer risk assessment. The FCA suggests that this means that first line employees often do not own or fully understand the financial crime risk faced by the firm, impacting their ability to identify and tackle potentially suspicious activity. It might, the FCA suggests, impact the independence of compliance. In other words, compliance cannot act independently in performing their role in relation to systems and processes that they are operating themselves. In these circumstances there is a risk of a loss of objectivity. The FCA concludes its comments on this topic by stating that in their experience, firms where those in business roles fully understand the relevant risks and know that part of their role and responsibilities is to help mitigate those risks, are significantly better at mitigating risks than their peers.	Firms should review the overall governance arrangements relating to the AML function to ensure that the structure is appropriate. This is particularly important in the context of the Senior Managers Regime and responsibility of individual senior managers for this issue.

(b) Ownership of key controls: Overseas firms

The FCA's concerns in relation to the ownership of key controls arises in relation to UK regulated branches or subsidiaries of overseas firms.

Most internationally based organisations will rely on their home jurisdiction and/or group-wide AML policies, procedures and processes. These will require appropriate domestication for UK legal and regulatory purposes to ensure that these are fit for purpose in the UK.

The FCA states that in principle there are no issues with this type of approach stating that this is "an acceptable practice when done well". The FCA goes on to emphasise the need for the UK branch or subsidiary to assert appropriate independence and involvement in these processes to ensure that that branch or subsidiary is operating in a manner that is compliant with UK requirements.

The FCA states that they have found that firms are often reliant on ready-made controls, frameworks, and products so that senior management of the UK branch or subsidiary are unable to demonstrate the assurance work undertaken regarding the effectiveness of those processes, or to evidence an adequate assessment of whether they fit with the UK entity's business model and risk exposure or UK laws and regulatory requirements.

The examples of the issues that may arise which are cited by the FCA include:

- Use of centralised sanctions screening or transaction monitoring capabilities and alert handling, meaning that the UK firm might not have visibility over the scope of these processes.
- In one firm the FCA was informed that the UK branch had no oversight of the transactional data fed into its transaction monitoring system and lacked management information to verify that the transaction data input at group level was complete, accurate or segmented appropriately.

The FCA states as good practice that firms appreciate that "one size" does not "fit all" and should ensure any systems or controls which are not bespoke are reviewed and tailored to the financial crime risks within their firm, branch or subsidiary. The FCA also refers to the fact that branches of overseas banks and their senior management must have a sufficient understanding of their UK regulatory responsibilities.

	(c) Senior Management sign-off The FCA refers to the fact that senior management approval and sign-off is required in some high-risk scenarios. For example, under Regulation 35 of the MLR senior management approval of is specifically required where a firm intends to establish a business relationship with a PEP. The FCA notes, however, that firms do not always evidence this level of governance. Whilst the FCA's Dear CEO Letter labels this section as "Senior Management Sign-Off", in fact the concerns that the FCA raises relate to broader governance issues so that firms can demonstrate that they have appropriate systems and controls to identify and manage AML risks. In relation to these matters the FCA states: • Where higher risk factors are identified or where approval of senior management is mandated, good practice involves firms having a governance committee responsible for key decision making on matters such as material financial crime related escalations and customer sign-off at on-boarding and at periodic review. • Where lower risk is determined and senior management sign-off is not mandated, the FCA would expect to see evidence of the first line of defence's assessment and rationale for acceptance at on-boarding and at periodic review. • The FCA refers to the fact that it has previously taken enforcement action where firms' governance arrangements were not adequately designed or effective.	
2. Business-wide risk assessment ("BWRA")	Under Regulation of the MLR firms are under an obligation to take appropriate steps to identify and assess the risk of money laundering and terrorist financing to which its business is subject. The Dear CEO Letter feeds back that the quality of the BWRAs the FCA has reviewed is poor. The issues include: • There is insufficient detail on the financial crime risks to which the business is exposed. • Firms have not adequately evidenced their assessment of the strength of the mitigating controls or recorded their rationale to support conclusions drawn on the level of residual risk to which the firm is exposed. • For overseas firms, the FCA raises concerns in relation to BWRAs completed at the group entity level which do not cover specific risks present in the UK, and which require a separate risk assessment.	Risk assessments should be reviewed. There is an obligation in any event for risk assessments to be kept up to date under the MLR (Regulation 18(3)).

3. Customer risk assessment ("CRA")	The risks arising in relation to individual customers also need to be managed. Firms will have risk scoring methodologies which will allow them to assess the risks relating to particular customers and then apply the appropriate level of customer due diligence and monitoring. For example, under Regulation 28(12) of the MLR firms must assess "the level of risk arising in any particular case" in complying with customer due diligence requirements. The FCA has found that CRAs are often too generic to cover different types of risk exposure which are relevant to different types of relationships. More specific concerns identified by the FCA include: • The failure by firms to differentiate between money laundering and terrorist financing risks, or the differing risks presented by a correspondent banking relationship as compared to a customer undertaking trade finance activity. • Discrepancies in how the rationale for specific risk ratings are arrived at and recorded by firms. • Lack of documentation recording the key risks and the methodology in place to assess the aggregate inherent risk profile of individual customers. • Failure to assess broader financial crime risks such as tax evasion or bribery and corruption.	Firms should ensure that they understand the basis of their customer risk assessment methodologies and that the methodology used is appropriate for the firm's business.

4. Customer due diligence ("CDD") and enhanced due diligence ("EDD")	A common failing identified in enforcement action taken by the FCA is that firms do not perform basic customer due diligence processes correctly. Aside from process and resourcing issues, many failings identified by the FCA in past cases have arisen from the failure by firms to identify and appropriately deal with higher-risk clients. As already noted above, the FCA focuses in its feedback on the importance of risk assessments as a foundation for AML processes. The Dear CEO Letter states that the FCA often identifies instances where CDD measures are not adequately performed or recorded. This includes seeking information on the purpose and intended nature of a customer relationship (where appropriate) and assessments of that information. In relation to Enhanced Due Diligence, the FCA states that it has identified that some firms' EDD is weak and does not always mitigate the risks posed by the customer. Concerns include: • Firms have identified a Politically Exposed Person ("PEP") relationship but do not evidence an adequate assessment of source of wealth ("SOW") and source of funds ("SOF"). • Firms do not always assess the level of risks posed by a PEP and tailor the extent of their due diligence, as required by Regulation 35(3) of the MLRs. • The FCA states that it has also found that firms confuse the purpose of obtaining SOW and SOF information, often requesting, obtaining and verifying the same documents to satisfy these two distinct requirements. This can lead to circumstances where the origin and legitimacy of a customer's wealth is not clearly understood or verified and/or the origin of funds accepted into an account at onboarding or throughout the relationship is unknown. • The FCA also emphasises the need for firms to assess whether SOW and SOF diligence should be performed even where this is not mandated under the MLR. The FCA notes that this is important to consider when applying the risk-based approach and implementing mitigants that address the risks. The FCA notes that the origins of a customer's monies are a key risk to the firm.	There is particular interest in the FCA's part in mitigating risks arising in relation to higher-risk customers. The FCA are also particularly concerned to ensure that firms focus on SOW and SOF issues both where this is specifically mandated (e.g., with PEPs) and in other higher-risk situations.

5. Transaction monitoring	The MLR contain a specific obligation for firms to have policies and procedures which provide the identification and scrutiny of: • transactions that are complex and unusually large, or where there is an unusual pattern of transactions; • transactions have no apparent economic purpose; and • any other activity or situation which the firm regards as particularly likely by its nature to be related to money laundering or terrorist financing. Transaction monitoring can be difficult to implement in practice. The FCA's Dear CEO letter raises the following concerns: • For branches and subsidiaries of overseas firms, group-led transaction monitoring solutions have not been calibrated appropriately for the business activities and underlying customer base of the UK regulated entity. UK firms must test whether the system is fit for purpose for the UK entity and where it is not, either tailor the system appropriately, or implement additional risk-based transaction monitoring measures. • Some firms' transaction monitoring systems are based on arbitrary thresholds, often using "off-the-shelf" calibration provided by the vendor without due consideration of its applicability to the business activities, products or customers of the firm. Firms need to consider and implement thresholds that are appropriate for their businesses and the relevant risks. Firms must be able to demonstrate an understanding of how transaction monitoring systems work and the data that they review. • The FCA specifically points to instances where firms have failed to assess alerted transactional activity against the established customer profile to validate the source of funds for high-value transactions.	Firms should ensure that they understand their transaction monitoring processes and these are appropriate for the firm's business and risk profile. The FCA is particularly concerned with systems that are bought from third party vendors who might themselves set escalation thresholds and other parameters. Firms must ensure that the systems used are objectively capable of identifying risks in their respective businesses.

6. Suspicious Activity Reports ("SARS")	The FCA raises a number of concerns in relation to the process for making internal SARs and managing situations in which concerns in relation to customers or transactions have been identified. • The FCA emphasises the need for firms to have documented policies in place to record the process by which firms' employees can raise internal SARs to the nominated officer. • Where there are concerns in relation to a customer, it is of course important to ensure that the customer is not "tipped off". In reviewing concerns, it will often be essential to interact with the customer directly but this must be done in an appropriate and careful way. The FCA points to a case it identified where a customer may have been alerted to money laundering concerns due to investigators not being appropriately trained in how to investigate potential suspicious activity. • A further concern raised by the FCA is that firms are unable to adequately demonstrate their investigation, decision-making processes and rationale for either reporting or not reporting SARs to the National Crime Agency ("NCA").	Firms should review their processes around the internal reporting of SARs and processes for documenting decision making in relation to the onward external reporting to the NCA.

4. Reporting suspicions of money laundering: Prosecution risk increases

4.1 Introduction

The reporting of suspicions of money laundering is an area that has received close scrutiny. The latest NCA SARs Annual Report states that in the period April 2019 to March 2020 a total of 573,085 SARS were made. The identification of suspicious transactions through monitoring processes and the review and reporting of transactions forms a large part of the £5 billion that UK institutions are estimated to spend annually on financial crime core compliance. The large number of SARs made has the potential to overwhelm the NCA. A large number of SARs could be regarded as being made on a defensive basis by institutions and there are long standing concerns around the quality of reporting, the Law Commission noted in its July 2018 Report on the SARs Regime that: "While reports of a high quality are being received, the SAR regime requires significant overhaul to improve the quality of financial intelligence available to the competent authorities... There are also concerns about the poor quality of some SARs across all reporting sectors. These concerns are recognised by the UK but have persisted for a number of years."

The large volume of SARs and concerns about their intelligence value have focused attention on how this can be managed and the volume reduced. At the same time and somewhat incongruously, it is clear that concerns remain that there is under-reporting at least in certain sectors. The Law Commission also referred to significant under-reporting by certain higher-risk sectors such as Trust and Corporate Service Providers, solicitors and accountants.

These concerns provide a context to the recent updating of the Crown Prosecution Service's ("CPS") Guidance on the prosecution of the failure to disclose suspicions of money laundering offence under the Proceeds of Crime Act 2002 ("POCA").

4.2 Reporting obligations

Regulated sector firms are subject to obligations to report suspicions of money laundering and terrorist financing both under the MLR and under the POCA.

Under Regulation 19(4)(d) of the MLRs firms are required to have policies and procedures in place to ensure that staff comply with Part 7 of POCA where they know or suspect or have reasonable grounds for knowing or suspecting that a person is engaged in money laundering. Part 7 of POCA of course includes the "Failure to disclose: regulated sector" offence (s.330 of POCA), whereby an offence is committed where a person working for a regulated sector firm fails to make a report, internally or externally, of suspicions of money laundering.

A number of prosecutions have been brought in respect of contraventions of s.330. These include, *R. v Swan and Woolf* [2011] EWCA 2275, which concerned operators of a safe deposit box business, *R. v McDonald* [2011] EWCA Crim 1776, which concerned a used car dealership, *R. v Griffiths and Pattison* [2006] EWCA 2115, which concerned solicitors and *Ahmad v HM Advocate* [2009] HCJAC 60, which concerned a money transmission business. These cases demonstrate the fact that successful prosecutions for breaches of s.330 have been brought. However, the cases have tended to focus on sectors and activities that might be regarded as peripheral. Of course, enforcement action brought by the FCA has resulted in sanctions being imposed on Money Laundering Reporting Officers ("MLROs"). For example, Steven Smith, who was Sonali Bank's MLRO and an SMF16 (compliance oversight), SMF17 (money laundering reporting), CF10 (compliance oversight) and CF11 (money laundering reporting), was fined £17,900 for failing to put in place effective systems for ensuring that staff were aware of their AML responsibilities and complied with their anti-money laundering obligations. Part of this related to the lack of SARs made by staff, particularly with regard to trade finance business. In fairness to Mr Smith, it is clear that the compliance and AML functions at the bank were under-resourced during the relevant period. Clearly, an effective reporting system is dependent on staff awareness of the responsibilities so that suspicions are escalated, and on an effective transaction monitoring system. Whilst the FCA recognised the resourcing constraints, this did not prevent the FCA taking action against Mr Smith personally (emphasising the need for MLRO to ensure that staffing and other resourcing concerns are appropriately escalated to and acted on by management).

While regulatory action has been taken in relation to contraventions of anti-money laundering obligations relating to SARs, criminal prosecutions have been more difficult with the CPS stating there have been 58 prosecutions in the period from April 2005 to September 2019 and 14 convictions.

4.3 CPS Guidance

On 2 June 2021 the CPS published its revised Money Laundering Offences Legal Guidance for prosecutors (the "Guidance"). The Guidance signposts a desire to encourage more prosecutions under s.330 of POCA for regulated sector firms failing to report suspicions of money laundering. The Guidance's focus is on whether prosecutions should only be brought where the underlying money laundering activities were planned or in fact undertaken. This emanates from statements made by the then Attorney-General, Lord Goldsmith, during a debate on the Proceeds of Crime Bill back in 2002. The scope of POCA and its proactive reporting obligations were controversial at that time. No doubt in order to provide some reassurance, Lord Goldsmith stated that "the offence in Clause 330 of failing to report to the authorities is permitted only if the prosecution proves that money laundering was planned or undertaken". The former Guidance by the CPS replicated this stating that "cases where this [s.330] offence is being considered should be referred to the Director's Strategic Policy Advisor at CPS Headquarters".

The Guidance now states that prosecutors may bring charges "even though there is insufficient evidence to establish that money laundering was planned or has taken place" noting that "there is nothing in the language of s.330(2) that required money laundering to be taking place". Given that s.330 imposes an obligation to report where there are merely reasonable grounds to suspect money laundering and does not specify that money laundering in fact must occur, this change to the Guidance appears to be legally justified. On the other hand, it is hard, though not impossible, to envisage circumstances in which a prosecution

would be brought for a failure to report suspicions when there was no underlying money laundering offence. It would be questionable whether it would be in the public interest in such circumstances to prosecute for a failure to report and moreover, if no money laundering in fact occurred, it would be more difficult evidentially to prove that there were reasonable grounds for a suspicion.

The CPS seeks to justify the change in its Guidance by relying on the Scottish case of *Ahmad v HM Advocate* [2009] HCJAC 60 which supports the approach that an obligation to report suspicions of money laundering arises regardless of whether money laundering in fact occurred. In the *Ahmad* case, the Court stated that "as matter of language it is obvious that a person may suspect that something is taking place, albeit it later turns out that his suspicion is ill-founded". While this may be so, as noted above, the merits of prosecuting an MLRO or other regulated sector staff member where there was no money laundering and any suspicions were wrong, is highly questionable.

4.4 Reporting where there is actual knowledge of money laundering

The above debate revolves around offences where there are "suspicions" of money laundering. However, the offence of failure to report can also be committed where there is actual knowledge of money laundering. Clearly, in these circumstances different considerations arise.

As to this, the Guidance states that: "evidence of planning or undertaking can support the prosecution in establishing the knowledge of the person that another is engaged in money laundering. Without such evidence of money laundering or planning, the prosecution will have to establish the suspect suspected or had reasonable grounds for suspecting money laundering."

4.5 Conclusion

The changes to the CPS Guidance certainly raise the stakes for MLROs and other employees of regulated sector firms. The benefits of prosecuting where there is no underlying money laundering are highly questionable. The very substantial number of SARs point to over-reporting and not under-reporting. To the extent that the quality of SARs needs to be improved, this could be achieved by regulated sector firms themselves.

5. FCA fines Sapien Capital in its first cum-ex trading case

5.1 Summary

On 6 May 2021, a boutique investment bank, Sapien Capital Ltd ("Sapien") received a £178,000 fine from the FCA (being reduced from £219,100 due to serious financial hardship) for failing to identify financial crime relating to cum-ex trading by Solo Group ("Solo") and their clients (whom Solo introduced to Sapien) during the period of 10 February 2015 to 10 November 2015. This is the first time the regulator has fined a party in relation to cum-ex trading, dividend arbitrage and withholding tax reclaim schemes.

Cum-ex trading is a method of rapid trading of securities around the dividend record date, which allows more than one withholding tax rebate to be claimed in respect of the same dividend payment. The value is therefore generated at a cost to the relevant tax authority, which pays out rebates in excess of the tax received. According to the FCA investigation, no change of ownership of the shares traded by the Solo clients, or custody of the shares and settlement of the trades by Solo took place, and in combination with the scale and volume of such trades, the practice was "highly suggestive of financial crime." The FCA believes the trades were undertaken to create an audit trail to support withholding tax reclaims in both Denmark and Belgium.

Sapien were found to have breached both Principles 2 and 3 of the FCA Principles for Businesses ("POB") for failing to have effective AML controls in place to detect such activity, as well as failing to ensure its employees exercised their roles with "due skill, care and diligence." This subsequently resulted in financial sanctions being imposed on them.

5.2 Facts and background of the case

In 2014, Sapien had taken on a new trading desk which conducted futures derivatives trades. The traders had previously acted for Solo at previous employers and arranged a meeting with Solo's representatives. However, at the meeting Sapien "was not informed of the nature or location of the clients, the volume of trading, or the trading strategy that they would employ" and yet, despite this, Sapien proceeded with a request to be added to Solo's broker list.

Sapien then proceeded to on-board 166 Solo clients despite a number of suspicious events during the on-boarding process including, among other things, mis-matching signatures, identical responses to many of the customer due diligence ("CDD") questions asked in their standard documentation and the fact that in total, only 15 people controlled all 166 Solo clients. Sapien also did not check the source of the funds from the Solo clients and incorrectly assessed that because it was not holding the clients' funds, it was not required to conduct such checks.

Sapien proceeded to execute trades in equity securities to the value of roughly £2.5 billion in Danish and £3.8 billion in Belgian equities over the course of February to November 2015. The trading pattern involved the use of Over the Counter ("OTC") equity trading, securities lending, and forward transactions, involving EU equities, on or around the last day securities were cum dividend.

5.3 Failings and sanction

The FCA found Sapien to have inadequate systems and controls in place to identify and mitigate the risk of being used to facilitate fraudulent trading and money laundering in relation to business introduced by Solo.

Principle 3 of the POB requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. Sapien were found to have breached this requirement because its policies and procedures were inadequate for identifying, assessing and mitigating the risk of financial crime where they failed to:

- give adequate guidance on how to conduct risk assessments and what factors to consider;
- set out adequate processes and procedures for enhanced due diligence ("EDD");
- set out adequate processes and procedures for transaction monitoring including how transactions are monitored, and with what frequency; and
- set out adequate processes and procedures for how to identify suspicious transactions.

In addition, Sapien staff were found to have not exercised "due skill, care and diligence" in accordance with Principle 2 of POB, in applying AML policies and procedures, and in failing to properly assess, monitor and mitigate the risk of financial crime in relation to the Solo clients and the purported trading.

Notably, they failed to carry out, among other things, the following key AML procedures:

- properly conduct CDD in accordance with their own policies and had amended CDD forms in response to complaints from Solo's clients that they required too much information;
- gather information to enable it to understand the business that the Solo clients were going to undertake, the likely size or frequency of the purported trading or the source of funds for the majority of the clients;
- document a risk assessment for each of the Solo clients;
- conduct EDD despite not physically meeting the Solo clients and the fact that entities with a net worth of less than €2 million were purportedly going to execute 25 trades of €100 million;
- conduct transaction monitoring of the purported trades of the Solo clients; and
- recognise numerous red flags.

As a result of Sapien agreeing to resolve all of the issues of fact and liability levied against it, Sapien had a 30% discount reduced further from £219,100 down to £178,000 in consideration of their position of "serious financial hardship."

5.4 Conclusion

Mark Steward, Director of Enforcement and Market Oversight, stated: "These transactions ran money laundering and other financial crime risks which Sapien incompetently failed to see."

"The FCA expects firms have systems and controls that test the purpose and legitimacy of transactions, reflecting scepticism and alertness to the risk of money laundering and financial crime, and failures here constitute serious misconduct."

This case may be an indication as to the future intentions of the FCA and its objective in cracking down on failings by firms to implement effective AML strategies. The FCA stated that its "investigation into the involvement of UK based brokers in cum/ex dividend arbitrage schemes is continuing."

6. Digitisation and decentralised finance

The last year has witnessed the growth of the digital asset sector, which has certainly now entered the mainstream. The use of cash has of course diminished through the COVID crisis. According to the Bank of England, in 2017 debit cards overtook cash as the most common method of payment in the UK. The number of cash transactions in the UK has decreased from 21.4 billion cash transactions in 2009 to approximately 9.3 billion transactions in 2019. In 2019, 2 million people mainly used cash for day-to-day transactions. However, this will certainly have declined in the COVID world. For example, in 2019 cash accounted for 27% of in store face to face transactions, whereas in 2020 use fell to 13% of transactions. The COVID crisis has clearly accelerated a latent trend.

The fall in cash use and migration of transactions to on-line environments has been accompanied by the increased prominence of digital forms of money, both private and governmental. Central Banks around the world have launched projects to develop Central Bank Digital Currencies ("CBDC") and some of these are in pilot phases. For example, the Riksbank in Sweden has been conducting a pilot for a CBDC e-krona. Whilst no decision has been taken to launch this outside the pilot, the Riksbank states that the purpose of the pilot is to increase its knowledge of the product, how this could be designed and what technology should be used. In the UK the Bank of England has announced the creation of a CBDC Taskforce which will co-ordinate work on exploring the introduction of a UK CBDC which has already been nick named "Britcoin".

The introduction of a CBDC will have a profound impact on a nation's payment and banking system. A system based on a central bank (blockchain) ledger will be introduced which will replace or run parallel to the existing payment and settlement system. Banks could be disintermediated and their source of funding removed. The digital currency itself could be programmed, for example, to expire after a set period of time or blocked from certain use. The implications will be great and will demand a greater involvement of the central bank. For money laundering and financial crime practitioners, the landscape will change as money and transactions are increasingly digitised.

Of course, private sector digital currencies are already in existence and use. Over the last year the price of Bitcoin, rather like the Grand Old Duke of York, has marched up to the top of the hill and almost back down again. On 17 June the FCA published a statement summarising the findings of its research on use of cryptoassets. This research showed that around 2.3 million in the UK own cryptoassets, up from around 1.9 million in 2020, and that 78% of adults have now heard of cryptocurrencies. The growth of the sector has been accompanied by increased regulatory scrutiny and proposals for a new regulatory framework. In the UK the Government has consulted on the UK's regulatory approach to cryptoassets and stablecoins while in the European Union the Commission has published a proposal for a Regulation on Markets in Crypto Assets.

In the meantime, the EU's Fifth Money Laundering Directive has entered into force. Amongst other things, this has required crypto exchanges and custodial wallet providers to register for anti-money laundering supervision purposes. Firms were originally required to register with the FCA by 16 December 2020. The FCA extended the Temporary Registrations Regime ("TRR") for existing cryptoasset businesses from 9 July 2021 to 31 March 2022. The TRR was established in 2020 to allow existing cryptoasset firms that applied for registration before 16 December 2020, and whose applications are still being assessed, to continue trading. In a statement issued in June, the FCA stated that: "A significantly high number of businesses are not meeting the required standards under the Money Laundering Regulations. This has resulted in an unprecedented number of businesses withdrawing their applications. The extended date allows cryptoasset firms to continue to carry on business while the FCA continues with its robust assessment." The FCA's statement highlights the challenges faced by hitherto unregulated businesses in bringing their systems and controls up to the level required for supervision by the FCA for anti-money laundering compliance purposes.

The digital assets world is evolving rapidly, and focus has shifted quickly to the world of "De-Fi" (decentralised finance) also referred to as open finance. De-Fi attempts to operate outside the existing financial system altogether. It is decentralised and not tied to any geographic location. It challenges current concepts and regulatory structures because of this. For example, crypto-currency exchanges can be regulated as they operate from physical establishments, use mainstream bank accounts and offer their customers to hold fiat currency balances and will convert crypto-assets to fiat. Often, a crypto-exchange will be registered for AML compliance under the Fifth Money Laundering Directive and also be authorised by the FCA as an Electronic Money Institution to enable them to provide accounts to their clients. Examples of De-Fi platforms include Aave which allows holders to crypto-currencies to earn fees from lending their crypto through the platform and Uniswap.

A major issue from an AML perspective is how these platforms are characterised; whether they are within the regulated sector and, if so, which parties involved in the platform should be subject to regulatory requirements.

De-Fi platforms will, of course, have founders who will develop the platform. However, De-Fi platforms are not operated or run in the sense that a traditional business is. The founders effectively establish the rules, develop the self-executing smart contracts and then let the system run. Decisions in relation to the operation of the platform are taken by a Decentralised Autonomous Organisation ("DAO") in which members of the platform participate. This could be, for example, members who hold governance tokens or generally native tokens on the De-Fi platform. However, no one person or entity might be regarded as being "in charge" of the platform.

De-Fi platforms are fundamentally peer-to-peer. Transactions do not depend on the role of an intermediary. For example, they do not depend on a central exchange or clearing entity. Moreover, transactions on De-Fi platforms do not use fiat currency. Instead, all transactions take place using crypto-currencies such as Ether (the native token of the Ethereum blockchain).

These features mean that De-Fi platforms can fall outside the scope of traditional regulatory and supervisory structures. They can of course, pose material AML and CTF risks.

In the US, the Securities and Exchange Commission ("SEC") has sought to challenge the concept that De-Fi platforms fall outside the scope of traditional regulation because of their decentralised nature. In March 2021 the SEC filed a complaint against LBRY, Inc, a decentralised business which founded the LBRY Network, a decentralised platform on which certain transactions in tokens took place. The SEC alleged that the tokens, called LBRY Credits, were securities and were offered to US investors in contravention of US securities laws. In its complaint the SEC alleges that LBRY sold more than 13 million LBRY Credits. LBRY, Inc., the Defendant legal entity, takes the position that it was not responsible for the relevant activities, on the basis that the platform on which the transactions took place was a decentralised platform. The SEC has challenged LBRY's position that it was a decentralised platform on the basis that LBRY maintained

managerial and entrepreneurial control over the LBRY Network, continued to control the software code for its applications and the protocol, took strategic and managerial decisions about the LBRY Network and took unilateral decisions as to how to allocate capital and resources it had pooled from investors. In other words, that LBRY was involved in sufficient centralised activities to be responsible for the activities on the platform.

Given these developments, the Financial Action Task Force ("FATF") has looked specifically at De-Fi and issued updated guidance on Virtual Asset Service Providers (FATF's draft guidance on a risk-based approach to virtual assets and virtual asset service providers of March 2021).

In October 2018, FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets. The effect of this was to require AML and CTF regulation to be extended to Virtual Asset Service Providers ("VASPs") including the regulation and supervision of providers of such services.

The amended FATF Guidance specifically address Peer-to-Peer ("P2P") business models such as De-Fi platforms. In relation to this FATF states that P2P transactions are Virtual Asset ("VA") transfers conducted without the use or involvement of a VASP or other obliged entity, such as VA transfers between two unhosted wallets. FATF recognises that P2P transactions are not explicitly subject to AML/CFT obligations under the FATF Recommendations. This is because the FATF Recommendations generally place obligations on intermediaries between individuals and the financial system, rather than on individuals themselves with some exceptions, such as requirements related to targeted financial sanctions. FATF recognises in its guidance that P2P transactions could pose heightened money laundering and/or terrorist financing risk, as they can potentially be used to avoid the AML/CFT controls imposed on VASPs and other regulated sector firms. The ability to conduct transactions without the involvement of a regulated intermediary was noted as a particular concern which FATF recognises challenges the effectiveness of traditional regulations.

FATF states that P2P platforms can still fall within the definition of a VASP and therefore be subject to AML regulation based on a broad reading of the definition of a VASP. FATF emphasises that a functional approach must be taken to determining whether a party is providing VASP services and that firms should not rely on a self-description by the provider or focus on the technology being used. FATF goes on to state that: "Only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and issuance will generally not be a VASP. For example, this may include websites which offer only a forum for buyers and sellers to identify and communicate with each other without offering, even in part, those services which are included in the definition of VASP." This represents a rejection by FATF of the notion that De-Fi platforms can be truly unintermediated or decentralised (i.e., that someone will always perform a centralised role and that person can be regulated).

In relation to determining who the VASP is in a De-Fi platform, FATF states that: "These applications or platforms are often run on a distributed ledger but still usually have a central party with some measure of involvement, such as creating and launching an asset, setting parameters, holding an administrative 'key' or collecting fees. Often, a [De-Fi] user must pay a fee to the [De-Fi], which is commonly paid in VAs, for the ultimate benefit of the owner/operator/developer/community in order to develop/run/maintain the software. [De-Fis] can facilitate or conduct the exchange or transfer of [Virtual Assets]".

While innovation continues apace, these developments make it clear that regulators and governments around the world will not permit the development of a parallel financial services system that sits outside traditional regulatory structures. The AML and CTF risks of permitting this to happen are, of course, high and we can all expect further enforcement and supervisory action to bring the De-Fi world into the regulatory net.

7. 7 Sustainable investment, ESG and money laundering

7.1 Introduction

Environmental, Social and Governance ("ESG") compliance seems a long way from the world of anti-money laundering and financial crime. ESG is closely linked to environmental issues and climate change. However, the "G" part of the acronym is an important component of the ESG concept. An organisation with good governance will ensure the delivery of environmental and social objectives and good governance is a sensible end in itself. Addressing illicit flows of money and preventing corruption are also key aspects to achieving sustainable development goals more generally.

7.2 Sustainable development goals

Until recently, ESG requirements have taken the form of "soft-law", that is non-binding requirements which have been derived from supra-national initiatives. The key foundation stone for ESG has been the UN Sustainable Development Goals ("SDGs"). These are 17 Goals ranging from ending poverty to promoting sustainable use of the terrestrial ecosystem. While these goals can seem lofty and perhaps not easily achievable, they are undoubtedly worthwhile and provide a policy framework to understanding many current legal and regulatory developments, including in relation to money laundering compliance.

The UN's Roadmap for Financing the 2030 Agenda for Sustainable Development 2019–2021 specifically refers to anti-money laundering compliance. It proposes engagement with global, regional and national policy makers and relevant stakeholders to create linkages between policies to combat illicit financial flows and financial development (including by strengthening the UN's existing relationship with the Financial Action Task Force). It goes on to stipulate that the UN should advocate with leaders from countries that receive illicit outflows to help prevent these financial streams, assist in repatriating illicit funds, and prosecute perpetrators. The Roadmap also recognises that anti-money laundering can play a role in preventing environmental degradation.

There are many aspects of the current anti-money laundering regime that are consistent with these objectives. For example, the focus on PEPs, their source of funds and source of wealth are directed in part at the potential abuse by PEPs in developing countries of their positions. Corruption, while of course not confined to developing nations, can act as a material hindrance to the achievement of the SDGs in developing countries. The focus on transparency of beneficial ownership and offshore jurisdictions associated with tax evasions are also key ways in which anti-money laundering compliance can support the SDGs. Efforts in the UK to tackle corruption through anti-money laundering laws and tools such as unexplained wealth orders support sustainability goals.

7.3 Sustainable finance disclosure regulation

The reliance on soft law has changed recently and rapid developments in this area are expected to continue apace.

In March 2021, the EU's Sustainable Finance Disclosure Regulation ("SFDR") came into force. The SFDR requires various European investment businesses and insurers to make public disclosures around their ESG compliance at an institutional level and at a product level. The SFDR is not part of retained EU law following Brexit and the end of the transition period. However, UK firms that market products into the EU/EEA or have EU/EEA based clients or investors are likely to be caught indirectly by its provisions. In any event, similar obligations are being introduced in domestic UK law, as is explained below.

In relation to financial products, the SFDR requires pre-contractual product disclosures to be provided to investors and also periodic ongoing reporting on sustainable investment issues. The idea is that the SFDR will result in investment being channelled towards sustainable investments and products. Investors will

carry out more detailed due diligence on investments for the purpose of assessing ESG compliance. For example, a private equity fund making an investment will need to carry out due diligence on the investee company on ESG compliance and also consider how it will exercise its stewardship responsibilities once the acquisition is made in order to further ESG aims.

Under the SFDR, firms in scope need to consider and provide disclosure in relation to whether they take account of sustainability risks in their investment decision making processes and the potential impact of those risks on financial performance of the investment. Sustainability risk for these purposes cover an environmental, social or governance event or condition that, if it occurs, could cause an actual or potential material negative impact on the value of the investment. Disclosure also needs to be provided in relation to whether the firm considers the principal adverse impact of investment decisions and advice on sustainability risk factors which cover environmental, social and employees matters respect for human rights and anti-bribery matters. The sorts of issues that firms must consider in determining the principal adverse impact of investment decisions include:

- Human rights issues such as human trafficking, forced and compulsory labour and exposure to controversial weapons such as land mines and cluster bombs.
- Anti-corruption and anti-bribery issues ("ABC") including, for example, an investee company's ABC policies, whether the investee company has failed to take sufficient action to address breaches of ABC requirements and enforcement action taken in relation to ABC matters.

7.4 UK initiatives

In the UK the FCA is presently consulting on Enhancing Climate Related Disclosures by Asset Managers, Life Insurers and FCA Regulated Pension Providers (CP21/17). The FCA's proposals are similar in nature to the requirements under corresponding EU legislation but are much more focused on environmental and climate change issues as opposed to broader ESG concerns.

7.5 FATF and environmental crime

It is in this context that FATF published its Report on Money Laundering from Environmental Crime (July 2021) ("Report"). The purpose of the Report is to take stock of the current methods that criminals are using to launder their gains from environmental crimes, enhance national authorities' and private sector awareness of the scale and nature of money laundering risks arising from environmental crimes identify priority actions at the national and international level to help combat criminal gains from environmental crimes, including potential regulatory or policy considerations.

In this Report FATF states that environmental crime is estimated to be among the most profitable proceeds-generating crimes in the world, generating around $110 to $281 billion in criminal gains each year. Around two third of this is derived from forestry crime, illegal mining and waste trafficking. FATF notes that "environmental crime has far reaching impacts beyond the financial cost, including for the planet, public health and safety, human security, and social and economic development. It also fuels corruption, while converging with other serious crimes such as drug trafficking and forced labour". Clearly, this language is redolent of ESG issues and dovetails with initiatives in the SDG and ESG sphere.

While there is no universal definition of environmental crime, it generally refers to criminal offences harming the environment. FATF's Report focuses on money laundering from select environmental crimes, which include illegal logging, illegal land clearance, illegal mining and waste trafficking due to the significant criminal gains involved, and their convergence with other serious crimes.

FATF's Report identifies the following key priorities:

- All Members of the FATF Global Network should consider whether criminals may be misusing their financial and non-financial sector to conceal and launder gains from environmental crimes. This includes countries without domestic natural resources.

- Members must also strengthen their operational capacity to detect and pursue financial investigations into environmental crimes. This includes working with foreign counterparts to share information, facilitate, prosecutions, and the effective recovery of assets that are moved and held abroad.
- Countries should fully implement the FATF standards as an effective tool to combat money laundering from environmental crime. This includes ensuring AML outreach to relevant intermediaries covered by the FATF Standards, such as dealers in precious metals and stones and trust and company service providers.

It is clear that there will be more focus on environmental crimes. Whilst the UK does not have a material natural resources industry, as a global financial centre the UK is vulnerable to money laundering in connection with the proceeds of such crimes.

8. A painting, a sculpture, or proceeds of crime? HMRC designates the UK art market as "attractive for money launderers" in first money laundering assessment on art market participants

On 28 June 2021, HMRC published its first ever money laundering risk assessment on art market participants ("AMPs") (the "AMP Risk Assessment") which lays down general money laundering risk indicators and risks specific to AMPs. Notably, HMRC currently assesses AMPs as high risk for money laundering, and art to be "attractive for money launderers" as art is likely to be less suspicious to law enforcement than, for example, gold or cash. Art is often sold on very international markets and sales are frequently facilitated through the use of third parties.

8.1 Background

The Fifth Money Laundering Directive brought AMPs into the scope of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLRs") where they fall within the statutory definition:

> "a firm or sole practitioner who (i) by way of business trades in, or acts as an intermediary in the sale and purchase of, works of art and the value of the transaction, or a series of linked transactions, amounts to 10,000 euros or more; or (ii) is the operator of a Freeport when it, or any other firm or sole practitioner, by way of business stores works of art in the Freeport and the value of the works of art so stored for a person, or a series of linked persons, amounts to 10,000 euros or more."

Whilst AMPs have long been subject to requirements to prevent and report suspected money laundering under the Proceeds of Crime Act 2002, the changes to the MLRs essentially bring AMPs into the regulated sector, subjecting it to regulatory supervision by HMRC. Prior to 10 January 2020, when the changes to the MLRs took effect, only AMPs that fell into the definition of "high value dealer" under the MLRs—essentially any business or sole trader that accepts or makes high value cash payments of €10,000 or more in exchange for goods—were subject to the MLRs. Now, however, all AMPs that fall into the statutory definition are subject to the general requirements of the MLRs and must:

- register with HMRC by 10 June 2021;
- carry out a risk assessment and maintain appropriate policies and procedures, and train staff appropriately;
- carry out customer due diligence and keep appropriate records of the same; and
- appoint a nominated officer and report suspicious transactions.

Whilst the above requirements will be familiar to many practitioners and businesses that have long been in the regulated sector, they will be new to most AMPs. The British Art Market Federation therefore published extensive guidance, approved by HM Treasury, on the new rules applicable to AMPs, which includes helpful art market-specific examples and case studies.

8.2 What is art?

Perhaps to the dismay of art critics everywhere, the MLRs have answered (or attempted to answer) the age-old question of whether something constitutes art by adopting the definition of "work of art" laid down in s.21 of the Value Added Tax Act 1994. According to s.21, the following are deemed to be "works of art":

- all hand-executed paintings, drawings, collages;
- unique or limited edition original engravings, lithographs or other prints;
- any original sculpture or statuary;
- limited edition sculpture casts;
- hand-made, unique or limited edition tapestries;
- hand-made, signed unique or limited edition ceramics;
- hand-made, signed unique or limited edition enamels on copper (excluding jewellery); and
- signed limited edition photographs (in editions of less than 30 for the same exposure).

However, the following are not deemed to be "works of art": (i) a technical drawing, map or plan; (ii) any picture comprised in a manufactured article that has been hand-decorated; and (iii) scenery (including backcloths).

This means that AMPs, which can include, for example, art dealers, galleries or auction houses and agents and intermediaries, that deal in "works of art" are subject to the requirements of the MLRs.

8.3 Specific art sector risks

The UK National Risk Assessment 2020 ("UK Risk Assessment") covered AMPs for the first time and noted that the UK art market, estimated to be worth around US$14 billion, is particularly attractive to criminals because sellers and buyers of art frequently wish to remain anonymous. Whilst there may be legitimate reasons for anonymity, this practice may be misused by criminals to conceal the ultimate beneficial owner and / or conceal criminal proceeds. In addition, the range in value of different art pieces means that the art market is attractive to varying levels of criminals, providing options to launder small and large sums of money. Whilst the most expensive pieces may attract careful, and often public, scrutiny, including tracing the history and ownership of the art, the majority of transactions will attract much less attention. This, coupled with the highly international nature of the art market, which means that pieces frequently move between jurisdictions, means that the art market is highly attractive for money launderers.

The risks pertaining to the art sector were also covered in the Amber Alert on AMPs, issued by the National Crime Agency and the Joint Money Laundering Intelligence Taskforce in May 2021 ("Amber Alert"). Reiterating many of the same risk factors as the UK Risk Assessment, the Amber Alert also stressed that most AMPs have not previously been subject to the MLRs and that full supervision and adherence to the regulations will take time. The fact that art is easily transportable further increases its appeal to money launderers. The Amber Alert also points to the fact that many recent money laundering and compliance scandals involved art. For example, the 1MDB scandal saw art included in US civil forfeiture proceedings.

8.4 AMP risk assessment

Given the classification of AMPs as high risk for money laundering, the AMP Risk Assessment stresses that businesses ought to carefully consider specific risks pertaining to their business in particular, and keep up-to-date policies, controls and procedures to prevent money laundering or terrorist financing. However, the AMP Risk Assessment identifies the following cross-sector risks for all AMPs:

Unusual sales or purchase activity: A potential sale or purchase does not appear to be normal business practice, have a valid commercial reason or make economic sense. AMPs should enquire about the reasons for the purchase as criminals may seek to take advantage of unwitting legitimate businesses. AMPs should also consider whether there is anything unusual about the manner or address to which the artwork is to be delivered.

Anonymity: The art market has a tradition of utilising third parties or facilitating auctions in private. This trading environment is advantageous to criminals seeking to conceal the proceeds of funds and / or the ultimate beneficial owners.

Payment from high-risk jurisdictions: The art market is very transnational, with parties often located in various jurisdictions, some of which are countries with poor / insufficient money laundering controls. AMPs need to decide on their level of comfort when assessing jurisdictional risk.

Remote sales: Online or phone transactions increase risks of money laundering by decreasing effective identification, particularly where the transaction is with a new customer.

Off-record sales: If a sale is conducted off-record, there will not be a proper audit trail. Off-record sales may also point to other risks, such as paying workers cash in hands and avoiding tax.

In addition, the AMP Risk Assessment notes that AMPs dealing with another AMP should check whether such AMP is registered with HMRC, and report if it is not. Due to the pandemic, there has been an increase in online and remote sales and AMPs are advised to conduct video calls to verify buyers and sellers. Lastly, HMRC clarifies in the AMP Risk Assessment that even interior designers and persons renting art could fall within the definition of an AMP if acting as an intermediary. All AMPs are therefore well-advised to carefully consider whether the MLRs apply to them, and heed HMRC's warning to "protect themselves, their families and their communities from the dangers of infiltration by criminals".

9. Ten years of the Bribery Act: Shifting the focus?

This section looks at whether the Bribery Act ("the Act") has, so far, lived up to its expectations. It will also discuss what the Act has meant for enforcement activity and the impact of deferred prosecution agreements ("DPAs").

9.1 An excellent piece of legislation

In March 2019, the House of Lords Select Committee on the Bribery Act 2010 ("the Committee"), published its post-legislative scrutiny report. The Bribery Act was described as "an excellent piece of legislation which creates offences which are clear and all-embracing." The corporate offence of failing to prevent bribery was regarded as particularly effective. Additionally, in 2017, the OECD, the principal source of pressure on the UK to modernise its laws, found that the UK had taken important steps to become a major enforcer of the foreign bribery offence among OECD countries and had demonstrated a strong anti-corruption drive.

9.2 The corporate offence of failing to prevent bribery

It is indisputable that the bribery offences under the Act are a vast improvement on their predecessors. However, the UK was also under pressure from the OECD to introduce a corporate criminal offence. This meant a departure from the conventional approach to corporate criminal liability by the inclusion of an offence under s.7 of failure of a commercial organisation to prevent bribery ("the corporate offence"). This offence, according to the Law Commission would "banish any doubt" over the adequacy of UK anti-bribery laws and compliance with obligations under international Conventions. It is a defence for a commercial organisation to prove that it had in place adequate procedures to prevent bribery by associated persons.

The Committee observed that because companies and their shareholders can benefit hugely from corrupt conduct, the question arose as to how they should be punished for what could be the conduct of a tiny minority of those involved, without harming those who have played no part. The Committee described the s.7 offence as "remarkably successful," so much so that the failure to prevent model was followed in the Criminal Finances Act 2017, in the creation of an offence of failure to prevent the facilitation of tax evasion.

9.3 Deferred prosecution agreements and the corporate offence

The corporate offence is proving to be the provision of the Act which has had the most significant impact. It undoubtedly put anti-bribery compliance on the agenda in an unprecedented way, but with the introduction of DPAs in 2014, it has also made investigating a corporate defendant far more attractive to law enforcement, which would otherwise have to rely on the "identification principle" to attach criminal liability to a corporate. The combined effect of the corporate offence and the DPA has provided a powerful weapon to the Serious Fraud Offence ("SFO"), currently the only UK agency to have used DPAs. For this reason, a discussion about the impact of the Act is almost inextricably linked to a discussion about DPAs and the corporate offence.

It is important to remember that DPAs apply to a number of criminal offences, but it is principally in relation to the corporate offence that they have been used. To date, six of the nine DPAs reached have involved the corporate offence. In July 2021, a tenth DPA is expected to be announced. It will be the seventh involving the corporate offence. In each case, the company has paid a large financial penalty, including in one case, a penalty of €997 million. With such huge paydays, it is no wonder that entering into a DPA with a corporate entity is an attractive prospect for the SFO and one on which it intends to focus.

9.4 Shifted focus?

In its Annual Business Plan for 2021/22, the Serious Fraud Office ("SFO") identified its key priorities. These include: "Encouraging good corporate compliance, and continuing to deploy [DPAs] where these can help to deliver justice for victims quickly and effectively, whilst mandating improvements to avoid future fraud, bribery or corruption." It is also worthy of note that the SFO also identified five outcome delivery measures against which to monitor progress. These tellingly include 'the total value of financial contributions to the government through the continued use of DPAs.'

The Committee, when it looked at the use of DPAs, also considered the prosecution of individuals. It emphasised in its report that the "DPA process far from being an alternative to the prosecution of individuals, makes it all the more important that culpable individuals should be prosecuted". In theory, the material provided to the SFO by a company as part of the cooperation expected in exchange for a DPA, should provide the evidence to assist in the prosecution of individuals. However, in every case where a company has entered into a DPA, the SFO has either unsuccessfully prosecuted individuals or not brought any charges at all. This raises another question about whether there is something amiss with the DPA process, the way it is being used or some other reason why this lack of success exists. It also raises the concern that the corporate offence has not had the enforcement impact intended. Has the realisation that DPAs provide a huge financial windfall distracted the SFO from its ultimate objective namely the investigation and prosecution of wrongdoing committed by individuals, or is there insufficient scrutiny of the underlying basis of a DPA? A DPA requires judicial approval before it can be finalised, however, a judge has limited insight into the granular detail of the basis of the proposed agreement between the SFO and the company, neither of whom, by the stage it reaches the court, has any incentive to derail the process.

The Director of the SFO has repeatedly stated in public that one of the difficulties faced by the agency in its pursuit of corporate defendants is the existence of the identification principle. The Law Commission is currently conducting a review of corporate criminal liability and is expected to report at the end of the year. However, this may not entirely explain the lack of success in convicting individuals. It may be that, with a DPA in its pocket, insufficient thought and scrutiny is given to the scope of the case brought by the SFO before it finds its way before the courts. It may also be that the DPA process is impacting the attention to detail applied in the disclosure process.

The perhaps unattractive conclusion may be that there has been a shift in focus, and as long as the SFO is able to produce bountiful DPAs, the absence of convictions of individuals will be overlooked. The fact that a measure of the SFO's progress towards achieving its priorities is the financial contribution DPAs make to the government may be a tacit acknowledgement that things have changed. It must be remembered that the SFO was, until relatively recently, an organisation facing disbandment. These continuing questions over the SFO's existence and its role in foreign bribery cases was a source of concern for the OECD which, it said could weaken the UK's progress in enforcement. However, the SFO's fortunes have changed and,

as it has previously boasted, as a result of DPAs, the SFO contributes more to the Treasury than it costs to run. It is interesting that the SFO is now working with a number of jurisdictions to share its experience in "successfully implementing the DPA regime".

9.5 A success?

There may come a time when, despite the income from DPAs, the public will be concerned about the absence of successful action against individuals and a consistent success rate will be expected. The corporate offence is a significant step in criminal liability of corporates but enforcement agencies such as the SFO must not lose sight of their purpose. DPAs are a good thing and are endorsed by the OECD. They provide a way for a company to resolve an allegation without a criminal conviction and for the SFO to obtain evidence and information it may otherwise not have been able to obtain. A DPA also encourages good corporate governance, is less costly than a trial against a large company and where appropriate can require continued monitoring of a company's compliance programme. According to the OECD, a DPA is an effective feature for incentivising self-reporting by companies and resolving foreign bribery cases against corporates. Despite this, most recently in 2019, the OECD observed that although there was an increased level of enforcement of foreign bribery, the total number of finalised and ongoing cases relative to the UK's economy remains low.

It is worth remembering that despite the attractiveness of the money brought in by DPAs, the SFO was created to address the problem of "the public no longer [believing] that the legal system of England and Wales is capable of bringing perpetrators of serious frauds expeditiously and effectively to book." In 1986, the Fraud Trials Committee in "the Roskill Report," which led to the creation of the SFO, found that the public's belief was right. The continued work of the SFO should be focused on this original concern.

Although the Act has been in force for 10 years, DPAs have been available for a shorter period and it may be that both require a longer period to marinate, as a pair, before any real impact can be seen.

10. UK gets tougher in penalising financial sanctions breaches: New OFSI guidance

10.1 Background

The UK Office of Financial Sanctions Implementation ("OFSI") recently published an update of its Monetary Penalties for Breaches of Financial Sanctions Guidance (the "Guidance") which came into effect on 1 April 2021.

Key issues for firms to consider are:

- OFSI's updated Guidance takes a broader approach to the territorial application of UK financial sanctions laws.
- Businesses or transactions with a more limited nexus to the UK might now be regarded by OFSI as falling within its remit.
- OFSI indicates that it will take a less tolerant approach where firms with otherwise good sanctions controls are involved in a contravention. A one-off breach is now more likely to result in formal enforcement action.
- OFSI stresses the need for full disclosure where a firm voluntarily reports a breach. An absence of full transparency may mean that a reduction in level of penalty will not be available in the case of voluntary disclosure.
- The tougher stance that OFSI sets out in the Guidance is consistent with more recent cases brought by OFSI, notably the £20.47 million imposed on Standard Chartered in February 2020.
- The introduction of new unilateral sanctions powers under the Sanctions and Money Laundering Act 2018 creates the potential of the UK imposing a broader range of sanctions (as it has already done).

For firms in the UK, the new Guidance highlights the need to have effective controls in place to comply with sanctions requirements. The combination of new legislation and a less benign enforcement environment means that the risks for firms have increased.

The updated Guidance clarifies how OFSI will exercise its powers to impose penalties for contraventions of sanctions requirements. These powers are conferred on OFSI by the Policing and Crime Act 2017 ("2017 Act") as amended by The Sanctions and Anti Money Laundering Act 2018, and OFSI can exercise these powers for breaches of financial sanctions.

10.2 Introduction to the guidance and on whom a penalty can be imposed

Chapter 1 of the Guidance introduces the basic information about financial sanctions and sets out the powers created by s.146 of the 2017 Act.

The most notable change to the introduction is the deletion of the wording in paragraph 1.22, which states that "OFSI will not normally impose a penalty on any person who has already been prosecuted". This deletion may indicate that OFSI intends to use monetary penalties in conjunction with other powers. Breaches of sanctions requirements are criminal offences which can be prosecuted. The above amendment to the Guidance indicates that OFSI might exercise powers to impose financial penalties even where the same party has been criminally prosecuted.

The remainder of para.1.22 is unchanged which leaves OFSI to use its discretion to impose a penalty on "one person involved in a case and for another to be prosecuted criminally".

10.3 Compliance and enforcement approach

OFSI confirms that it still intends to take a holistic approach in ensuring compliance with the UK financial sanctions regime, but it is worth noting the minor change to the language in para.2.2 of the Guidance, where OFSI states that it aims to provide messages its audience can "understand and respond to". The emphasis here is to ensure that the whole "lifecycle of compliance" is considered in an attempt to promote understanding of the guidance and to pre-empt potential breaches.

10.4 Case assessment

Chapter 3 contains the most wide-ranging changes to the Guidance compared with the previous version and indicates the tougher stance on enforcement that OFSI is taking. It provides an overview of the considerations that OFSI will take into account when assessing potential breaches.

Paragraph 3.2 sets out the steps that OFSI may take in response to potential breaches and now states that it "may undertake several of these actions in any particular case". This re-iterates the point implied by the deletion at para.1.22 (see above) and suggests it might impose a monetary penalty as well as refer the case to law enforcement agencies for criminal investigation for example. This is a notable change from the previous guidance.

The drafting around responses to potential breaches has also been tightened. Rather than "issuing correspondence requiring details of how a party proposes to improve their compliance practices", OFSI may now simply "issue a warning". This suggests a potential escalation in the relationship with firms where a contravention is identified and a greater likelihood that there will be an enforcement outcome, even if this is just a warning.

The changes made to the Guidance also suggest that OFSI will show a greater interest in matters with a non-UK connection. OFSI's previous Guidance stated: "We will not artificially bring something within UK authority that does not naturally come under it." This statement has now been deleted at para.3.8, which may suggest a greater desire to take on cases with a limited UK jurisdictional nexus and provide a wider scope under which OFSI may catch sanctions breaches. An example of this could possibly include payment flows through UK banks but it is still unclear the extent to which this wider net may be cast.

The Guidance has also removed wording that OFSI is "likely to treat a case that directly and openly involves a designated person more seriously than one that is a breach of financial sanctions but does not make funds or economic resources available to a designated person" (para.3.16). When read in conjunction with the lowering of the threshold for 'most serious' cases (see para.3.46), this might suggest a greater scope within which more individuals could be caught for breaches that are more serious.

OFSI will still consider the type of work a person does and "their exposure to financial sanctions risk" and "level of actual and expected knowledge" (para.3.20) when determining the action to be taken. However, the deletion of wording from previous guidance (at para.3.22) which suggested that a more lenient approach could be adopted if a person observing a high standard fell below that standard and acted swiftly to remedy the cause of the breach, would otherwise suggest that on balance a stricter, less forgiving approach may be forthcoming.

Furthermore, repeated, persistent or extended breaches will now be considered as an "aggravating factor", especially when the individual is unresponsive to such previous warning (para.3.26). The wording has become more forceful and suggests a tougher stance to those who do not respond to breaches appropriately, with the indication that all previous breaches will now be taken into consideration, rather than "tend to" as was previously drafted.

Disclosure requirements also seem to have become more onerous. Those self-reporting must report "all evidence relating to all the facts of the breach", as opposed to information that is "materially complete on all relevant factors". This removes the ability to decide one's own materiality threshold and requires all information be disclosed for OFSI to make such assessment for itself.

The threshold for 'most serious' type cases has been lowered where "blatant flouting of the law" has been replaced with "particularly poor, negligent or international conduct." Whether a breach is "serious" or "most serious" affects the monetary penalty amount imposed and so it is possible we may see higher penalties due to this rephrasing of the guidance.

10.5 The penalty process

OFSI states that it will still assess what level of penalty is "reasonable and proportionate" within the statutory maximum but there has been an amendment to the definition of "proportionate" at para.4.8 of the Guidance. The statutory maximum remains unchanged (i.e., it remains the greater of £1 million or 50% of the value of the breach), but there will now be "a holistic assessment of all the other factors present in the case" instead of the "value of the breach (if known) and how seriously the breach undermined the sanctions regime". This appears to give greater discretion to OFSI where it has plenty of scope in deciding what factors are relevant.

Voluntary disclosure continues to be encouraged with up to a 50% reduction in the final penalty amount if prompt and complete voluntary disclosure is given. However, OFSI also states that if there have been a series of breaches "where only some were voluntarily disclosed to OFSI", it "will take that into account when determining any reduction" in the potential penalty for the breach. Paragraph 4.10 makes clear that should there be a failure to make complete disclosure during an investigation (amongst other failures), this voluntary disclosure reduction may not be applied at all. This will be judged on a case-by-case basis and removes the automatic access to the voluntary reduction available previously. The effect this re-drafting has is to reward those who give full and complete voluntary disclosure, whilst removing access to a reduction for those who selectively disclose information simply to seek out a reduction.

Paragraph 4.11 now includes the provision that if there is an offence with no transaction value, OFSI will "impose such penalty as seems reasonable and proportionate to the facts of the case" whilst the permitted maximum for such cases is £1 million. This is a new addition to the guidance.

Paragraph 4.21 in the previous version of the guidance has also been removed from the latest draft. This is notable given that it provided OFSI with discretion not to impose a penalty in some scenarios such as where a penalty would have "no meaningful effect" or if it would be "perverse". Again, this could hint at a greater appetite for pursuing potential breaches by OFSI.

10.6 Procedure for imposing a penalty

The guidance on procedure has not changed much other than the granting of a longer period in which a person can make written representations. This has been extended from 28 calendar days to 28 working days. OFSI may also now consider and respond to such representations within 28 working days rather than calendar days.

10.7 The right of Ministerial review and paying a penalty

Section 147(3)(b) of the 2017 Act states that OFSI must inform the person upon whom it is imposing a penalty that they are entitled to Ministerial review. Such process and guidance largely remains unchanged in Chapter 6 with the exception that the timeframe for seeking such review has been extended from 28 calendar days to 28 working days and that HM Treasury will aim for such reviews to be concluded within two months as opposed to 28 calendar days.

A deadline has also been introduced at chapter 8, which imposes a 28-working day timeframe within which to pay monetary penalties once such penalty has been finalised and payable. This differs from the "reasonable time" within which to pay as previously indicated. Such timeframe starts from the date the penalty is imposed.

10.8 Publication of penalty details

In accordance with s.149(2) of the 2017 Act, the Treasury is required to publish reports about monetary penalties. Paragraph 9 of the guidance clarifies that the GBP value of the transactions which are in breach of the regulations will be aggregated if such GBP amount can be identified. This chapter has also been updated to clarify that the summary will only be published after the person has had the opportunity to exercise their right to Ministerial review. It also states that if there is an appeal to the Upper Tribunal and there is quashing or amendment to the penalty, OFSI will publish the amended information.

10.9 Conclusion

As can be seen from the above, it is apparent that the updated Guidance signals a tougher approach to enforcement by OFSI. The changes at Chapter 3 in particular signpost where it intends to expand the use of powers granted to it with responses to potential breaches no longer being mutually exclusive. It remains to be seen how the Guidance will be implemented but the practical effects on those subject to UK financial sanctions, especially those self-reporting, could be significant.

COMPLIANCE OFFICER BULLETIN

ProView

THIS TITLE IS NOW
AVAILABLE DIGITALLY

Thomson Reuters ProView

The Premier eBook experience for professionals worldwide
via your browser, tablet or smartphone

For further information and a free trial please select
Print Services in Contact us at www.tr.com/uki-legal-contact,
call 0345 600 9355, or contact your trade agent

Download on the App Store

GET IT ON Google Play

THOMSON REUTERS®

Issue 189

Data Protection, Cyber Resilience and Operational Resilience after Brexit

Authors: **Simon Stokes, Blake Morgan LLP**

Coverage

Data protection and cyber security remain in the news. The completion of Brexit means a new UK data protection regime modelled on the EU regime. In reality, pretty much as the same as the prior EU regime but nevertheless adapted for the UK. This has specific implications for cross-border data flows as the UK is now a third country as regards the EU. In addition, the 2020 decision of the CJEU in Schrems II is also relevant. At the same time regulators in both the UK and the EU are focusing on cyber resilience in the context of operational resilience more generally. In March 2021 the guidance and rules applied by the Bank of England, the PRA, and FCA in relation to operational resilience were finalised. These will come into force on 31 March 2022. The EU has also proposed a digital operational resilience framework for financial services ("DORA"). Issue 189 of Compliance Officer Bulletin will consider these developments, as well as providing an update on data protection compliance more generally.

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 18 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.

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C020438

42830038