THE CITY LIBRARY

ISSUE 178 – August 2020

COMPLIANCE OFFICER BULLETIN

Money Laundering and Financial Crime

The authors are all lawyers in **Paul Hastings**' London, Washington DC, and Paris Offices. They specialise in advising clients on financial services regulatory issues and also in dealing with money laundering and other complex financial crime issues. Attorneys from Paul Hastings regularly advise clients on the review and development of compliance policies and procedures. They also represent clients in regulatory and law enforcement investigations and proceedings and in litigation matters.

Arun Srivastava, Partner (London)

Nina Moffatt, Senior Associate (London)

Konstantin Burkov, Associate (London)

Zach Benson, Associate (London)

Gesa Bukowski, Trainee (London)

Tom Best, Partner (Washington DC)

Jonathan Drimmer, Partner (Washington DC)

Matt Herrington, Partner (Washington DC)

Nicola Bonucci, Managing Director (Paris)

1. Introduction

The recent weeks and months have been dominated by the COVID-19 crisis. Government and regulatory attention has focused on the impact of the crisis and measures that can be taken to alleviate the economic and financial impact of the crisis on consumers and businesses. The authorities have, however, been alert to the financial crime risks that have been generated by the crisis which firms must continue to manage and mitigate. There has also been continued enforcement activity with a number of prominent financial crime cases being concluded and publicised in the lock-down period. Firms must, of course, continue to have regard to the issue highlighted in these cases.

1.1 The Fifth and Sixth Money Laundering Directives

At the outset of the year, which now seems distantly far away, minds were focused on the transposition of the EU Fifth Money Laundering Directive. This was required to be implemented by 10 January 2020. The purdah period around the 2019 election meant that the Government did not have time to complete the consultation process. The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 amended the existing regulations to implement changes required under the Fifth Money Laundering Directive. The Fifth Money Laundering Directive has brought various

CONTENTS

THOMSON REUTERS™

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

ISSN: 1478-1964

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

HOW TO PLACE YOUR ORDER

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

By Phone
0345 600 9355 (UK)

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

activities in relation to the burgeoning cryptocurrency industry within the scope of regulation for anti-money laundering purposes. Specifically, crypto-exchanges and custodian wallet providers are now within scope. This will prove to be the first step in the path towards broader regulation of the crypto industry. The COVID-19 crisis, with its emphasis on on-line and non-face-to-face transactions will act as a catalyst for the digital asset industry. The figures for the growth of the industry were already impressive even before the crisis struck and now look to grow even more rapidly. The European crypto-currency market is expected to grow in size from US$5.165 billion in 2019 to US$15.263 billion in 2026.

Transposition of the Fifth Money Laundering Directive has lagged in some Member States of the EU. As at the beginning of June 2020, no transposition measures had been communicated by Cyprus, Portugal, Romania, and Spain. Partial transposition measures had been communicated by Austria, Belgium, Czech Republic, Estonia, Ireland, Greece, Hungary, Luxembourg, Netherlands, Poland, Slovakia, Slovenia, and the UK. Only 11 Member States, including France, Germany, and Italy, had communicated full transposition measures to the Commission.

The EU is also focused on its Sixth Money Laundering Directive and the EU's Money Laundering Action Plan. We cover the EU's Action Plan in detail in this Bulletin. The implementation of the Fifth Money Laundering Directive in the UK was required to take place shortly before the UK's departure from the EU (at the end of 2020). The extent to which the UK will shadow EU legislation in the future remains unclear at this time.

The objective of the Sixth Money Laundering Directive is to bring about consistency of approach across the EU towards criminal money laundering offences. It addresses the lack of a coherent approach across the EU to criminalisation of money laundering. The Directive:

- Defines criminal offences considered to be predicate offences (it lists 22 offences);
- Specifies minimum sanctions;
- Extends criminal liability to legal entities;
- As well as to natural persons holding a leading position who commit criminal offences for the benefit of the legal entity.

The 22 predicate offences listed include tax crimes, environmental crimes, fraud and cybercrime. In the UK, the Proceeds of Crime Act 2002 takes an all crimes approach and does not list out individual predicate offences. The UK Government takes the view that the UK is already largely compliant with the Sixth Money Laundering Directive. In any event, crimes of cheating the revenue (criminal tax evasion) fraud under the Fraud Act 2006 and cybercrime under the Serious Crime Act 2015 and the Computer Misuse Act 1990 are all crimes and predicate offences for the purposes of UK anti-money laundering legislation.

It should also be noted that since the UK had opted out from EU criminal law initiatives like the Directive (when the UK was still an EU Member State) and since we have now left the EU, the Sixth Money Laundering Directive is likely to be of little relevance to the UK.

1.2 Enforcement, Financial Sanctions and China

The COVID-19 crisis period has also seen a steady stream of enforcement cases emerging. Clearly, by the time fines and sanctions become public, investigations and enforcement cases will have been ongoing for many months if not years. We cover in this Bulletin the fine imposed on Commerzbank's London Branch for AML breaches. We also cover recent enforcement action by the UK's Office of Financial Sanctions Implementation against Standard Chartered Bank for breaches of financial sanctions obligations.

Financial sanctions are becoming even more topical given geopolitical events. The US has focused recent efforts on sanctions targets located in China. Steps taken in the United States include:

- The Uyghur Human Rights Policy Act of 2020 was enacted in June 2020. The Act confers power to imposed Magnitsky Act sanctions (i.e., for human rights abuses) against person involved in the mistreatment of the Uyghur population.
- On 21 May 2020 a Bill was introduced in the US Senate which would allow the US to impose sanctions on individuals and entities who violate China's obligations to Hong Kong. Importantly for banks, it would also allow the US to impose mandatory secondary sanctions on banks that do business with such individuals and entities. The was enacted with bipartisan support as the Hong Kong Autonomy Act on 25 June 2020.
- On 20 May, the US Senate passed a bill that would require US Government audit oversight of Chinese US-listed companies, and access to their audit papers—without which those companies could be de-listed—threatening to cut Chinese companies off from US capital markets.
- On 15 May, the US Department of Commerce (DOC) introduced a range of new restrictions on Huawei. Originally placed on the denied parties lists in 2019 because of dealings with Iran, the new restrictions address that company's alleged circumvention of those controls, but also are aimed to make it virtually impossible for Huawei to make semiconductors using cutting-edge US technology.

It is also worth noting that on 28 April, DOC tightened controls on exports to China, Russia, and Venezuela—significantly expanding the definition of "military end uses" for a wide swathe of US technology, and removing licence exceptions in the existing regulatory restrictions on exports to China in a way that will require the licensing of huge chunks of US–China outbound trade: Of course, those licence applications will be subject to a policy of denial in most cases

We cover later in this Bulletin the first use of new powers under UK legislation to impose Magnitsky style sanctions for human rights violations.

1.3 COVID-19 and FCA financial crime systems and controls

In relation to the COVID-19 crisis, national, EU and supra-national authorities have all issued statements and guidance around financial crime risks emerging from the COVID-19 Crisis.

In relation to this the FCA has stated that "Maintaining the integrity of the financial market is a key objective for the FCA. In the current climate, it is important for firms to maintain effective systems and controls to prevent money laundering and terrorist financing".

The FCA's statement highlighted the fact that criminals had already been taking advantage of the Covid-19 Crisis to carry out fraud and exploitation scams through a variety of methods, including cyber-enabled fraud. Firms were (and are) encouraged to submit suspicious activity reports around new typologies in particular.

The FCA has taken notice of the operational challenges presented by the COVID-19 Crisis, including of course remote working, the absence of staff from offices, the impact of this on operational systems and the furloughing of staff so that fewer are available to operate systems than in the pre-crisis period. Risks that have been identified include:

- Remote working creates a greater risk of cyber-crime given increased reliance on on-line access and remote systems. Firms are also less able to monitor staff conduct where personnel work remotely;
- Similarly, increased on-line consumer transactions as well as an increased use of social media and other platforms by customers, driven by the lock-down and continued because of social distancing measures, also create greater cyber-crime risks. Cyber-crime risks include risks of email and SMS phishing attacks (including government impersonation), business email compromise scams and ransomware attacks;
- The economic impact of the crisis with increased unemployment and lower economic activity will create new risks as new patterns of activity emerge;
- The Financial Action Task Force (FATF) has suggested that criminals will exploit economic stimulus measures and insolvency schemes as a means to conceal and launder criminal funds;
- FATF also points to an increased risk of the misuse and misappropriation of domestic and international financial aid and emergency funding. As well as criminal diversion of funds, this could also give rise to greater corruption risks involving public officials in third countries who are the recipient of financial aid;
- As noted customer and business behaviours might change creating new risks. These include the increased use of the informal or unregulated financial sector where financial crime controls are non-existent;
- FATF have also postulated that the current turbulence in economic activity might create the potential for criminals and terrorists to move into new cash-intensive and high-liquidity lines of business in developing countries;
- Restrictions on air and other travel has also caused disruption to criminal activity. This will displace such activities so that new methods of detection and supervision will be required given changes to typologies; and
- At the same time government and law enforcement have been required to reprioritise and devote more resources to dealing with the COVID-19 Crisis. This has meant that fewer resources are available to be deal with AML and other financial crime matters.

As well as concerns and risks around AML, the disruption of normal business processes and the volatility of financial markets also gives rise to the risk of market abuse and insider dealing in the financial markets.

Certain dispensations have been recognised explicitly including in relation to regulatory returns.

Undoubtedly, interesting supervisory and enforcement issues will emerge from the COVID-19 Crisis based around how firms have responded to event. The extreme real life stress testing that firms have undergone will in some cases exposure pre-existing cracks and fissures.

Although the FCA has been understanding of the issues that firms have had to deal with, they have also reinforced the message that firms cannot afford to take a more relaxed approach to compliance particularly where high-risk clients and business are concerned.

This message is supplemented through the Senior Managers and Certification Regime, which has applied across all FCA firms from December 2019. The FCA and PRA issued a Joint Statement on arrangements for senior management in dual regulated firms, and the FCA also published a statement for its solo-regulated firms. The statements confirmed the status of Senior Managers as key workers under Government lock-down related regulations. The PRA and FCA statements said that individuals performing required functions (including the Money Laundering Reporting Officer (SMF17)) should only be furloughed as a last resort.

Of course, under the SMCR individuals in Senior Management would have been allocated prescribed responsibilities that they will need to continue to fulfil and also discharge their statutory duty of responsibility. Again, some allowance has been made by regulators, so that the need to notify regulators of changes in prescribed responsibilities has been alleviated provided that the firm has kept appropriate written records of changes made. Whilst a degree of understanding has been extended to the regulated

community, it is also clear the roles, responsibilities and practical discharge of these will come under the microscope in cases of failure. The events relating to the failure of Wirecard, whereby around $1.9 billion in customer funds are reported to be "missing" once again show that when the tide goes out, incidents of misconduct are likely to be exposed. Firms and individuals who work in them must therefore remain focused on the financial crime and other risks as the situation develops.

2. Financial Sanctions: UK Government targets human rights contraventions

Foreign Secretary Dominic Raab has announced on 6 July that the UK Government is using new financial sanctions powers to target "buying property on the King's Road and shopping in Knightsbridge" from money siphoned from UK banks by individuals engaged in human rights violations.[1] The focus on property and shopping is of course designed to attract publicity and highlight the Government's actions. However, it does raise serious issues with regard to the susceptibility of the UK's financial system to facilitate laundering by those involved in corrupt and unlawful activities in their home jurisdictions.

Famously, UK authorities have already used powers to obtain Unexplained Wealth Orders including against Zamira Hajiyeva (who did indeed shop in Harrods). These powers were introduced under the Criminal Finances Act 2017. They have been used with mixed success with the Court in another case setting aside the use of the powers. We cover these issues in a separate section in this Bulletin.

The financial and immigration sanctions announced by the Government are the first ever sanctions under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA), targeting 49 Russian, North Korean, Myanmarese, and Saudi Arabian nationals and organisations. This section provides an overview of the law and examines the sanctions imposed.

2.1 UK Sanctions Regime under SAMLA

The individuals and organisations who are the targets of the Government's sanctions are accused of human rights abuses around the world. These sanctions are being imposed under the new regime set out in the SAMLA, which was originally passed into law to replace the EU sanctions regime post-Brexit.

2.1.1 Sanctions Background

The UK, as a member of the United Nations, is required to implement sanctions passed by resolutions of the UN Security Council. Such measures are implemented through EU Regulations that take direct legal effect in all EU member states. As sanctions regimes are evolving areas that need to adapt to the prevailing circumstances, the UK Government took the view, when considering the implications of Brexit, that merely transposing EU Regulations on financial sanctions into national law was not sufficient.

The UK has been "on-shoring" EU laws for around two years to take account of Brexit. Departure from the European Union means that EU laws will cease to apply in the UK. To minimise disruption, legislation has been passed to on-shore or domesticate EU laws to carry them across post-Brexit. This includes financial sanctions. This on-shoring has been achieved through SAMLA. However, new sanctions will need to be imposed and the Government will want to act unilaterally. Therefore, SAMLA contains new, wider powers for the UK to operate its own sanctions regime.

2.1.2 Key Features of SAMLA: When can sanctions be imposed?

SAMLA has two main purposes:[2]

1. To enable the creation of a national sanctions framework, where the UK can impose its own sanctions, as opposed to adopting EU and UN sanctions, for the following reasons:

(a) to comply with UN obligations or other international obligations;

(b) to further the prevention of terrorism;

(c) to secure national security or international peace and security;

(d) to further foreign policy objectives; and

(e) to provide accountability for or be a deterrent to gross violations of human rights.

2. To enable the updating of the national anti-money laundering and counter-terrorist financing regime by making provision for the purposes of the detection, investigation and prevention of money laundering and terrorist financing, and to implement standards published by the Financial Action Task Force (FATF) relating to combating threats to the integrity of the international financial system. The UK previously adopted EU directives.

Sanctions may be imposed if the UK Government considers them "appropriate" for one of the above purposes.

In addition, under SAMLA "an appropriate Minister" (which means the Secretary of State and the Treasury)[3] is permitted to make regulations to amend the SAMLA to authorise new types of sanctions when the Minister considers it "appropriate" to comply with UN sanctions or to further one of the grounds set out above. This wide power has been criticised as giving the Government unconstrained power and the ability to change legislation without involving Parliament.

The sanctions that were imposed on 6 July were indeed made under such regulations made by the Secretary of State: The Global Human Rights Sanctions Regulations 2020 (the "Global Human Rights Regulations") were laid before Parliament on 6 July 2020 and used to impose sanctions the same day. Under the Global Human Rights Regulations, sanctions can be imposed to deter, and provide accountability for activities (carried out outside the UK by any person or in the UK by a non-UK citizen) which, if carried out by or on behalf of a State within the territory of that State, would amount to a serious violation by that State of an individual's:

(1) right to life;

(2) right not to be subjected to torture or cruel, inhuman or degrading treatment or punishment; or

(3) right to be free from slavery, not to be held in servitude or required to perform forced or compulsory labour, whether or not the activity is carried out by or on behalf of a State.[4]

2.1.3 Key features of SAMLA: Designation of person on whom sanctions are imposed

To impose sanctions, the Minister must clearly identify and designate the individual or organisation on whom the sanctions are imposed. Controversially, SAMLA gives the Government the power to designate persons by "description" as well as by name.

To designate by description, the following conditions must be satisfied:

1. The description of persons specified is such that a reasonable person would know whether that person fell within it.

2. At the time the description is specified, it is not practicable for the Minister to identify and designate by name all the persons falling within that description at that time.

3. The Minister has reasonable grounds to suspect:

(a) that where the specified description is members of a particular organisation, that the organisation is an "involved person"; or

(b) in the case of any other specified description, that any person falling within that description would necessarily be "an involved person".

Designation by description raises obvious questions, such as if the description is so specified that "a reasonable person would know whether that person fell within it", why is the person not simply specified? It also creates uncertainty for organisations trying to ensure compliance and raises concerns that loose descriptions may be misused against the wrong individuals.

2.1.4 Key features of SAMLA: Types of sanctions

SAMLA grants relatively broad sanction-making powers as a range of sanctions may be imposed, such as financial or immigration sanctions, trade sanctions, and airport or shipping sanctions.[5]

Financial and immigration sanctions are likely to be the most commonly used form of sanctions when targeting individuals; indeed, those were imposed in the first ever sanctions made, discussed further below. As the financial and immigration sanctions under SAMLA are the same as the ones imposed under the Global Human Rights Regulations, these are discussed in more detail below.

2.1.5 First Sanctions Imposed

Following the poisoning of Sergei and Yulia Skripal in March 2018, perhaps better known as the "Salisbury Attack", and a campaign on behalf of the family of Sergei Magnitsky, the Russian lawyer beaten to death in Moscow in 2009 after uncovering embezzlement by high-ranking officials, a so-called "Magnitsky clause" was added to SAMLA. This clause, styled after the Magnitsky Act in the US, allows the Minister to impose sanctions to provide accountability for or deter gross human rights violations.

The UK Government has now announced that its first-ever sanctions under SAMLA are indeed targeted at individuals "who have committed the gravest human rights violations".[6] The sanctions against 49 named individuals and organisations from Russia, North Korea, Myanmar, and Saudi Arabia came into force immediately and freeze UK assets of those named as well as preventing them from entering the UK.[7]

The sanctions are targeting:

(1) 25 Russian nationals involved in the mistreatment and death of auditor Sergei Magnitsky, who uncovered widespread Russian corruption by a group of Russian tax and police officials;

(2) 20 Saudi nationals involved in the death of journalist Jamal Khashoggi;

(3) two high-ranking Myanmar military generals involved in the systematic and brutal violence against the Rohingya people and other ethnic minorities; and

(4) two organisations involved in the forced labour, torture and murder that takes place in North Korea's gulags.

2.2 Impact of sanctions on businesses

2.2.1 Offences created

The Global Human Rights Regulations provide that a person (which includes a corporate body) must not:

(1) deal with funds or economic resources owned, held or controlled by a designated person;

(2) make funds available directly or indirectly to a designated person;

(3) make funds available to any person for the benefit of a designated person;

(4) make economic resources available directly or indirectly to a designated person; and

(5) make economic resources available to any person for the benefit of a designated person;

if the person knows, or has reasonable cause to suspect, that they are dealing with such funds.[8]

In addition, a person must not intentionally participate in activities knowing that the object or effect of them is to circumvent, or enable or facilitate the circumvention of, the Global Human Rights Regulations.[9]

Getting compliance right is important for businesses and their employees and officers (which can be held liable for the actions of a body corporate if the activity was committed with the director's consent or is attributable to their negligence)[10] as the Global Human Rights Regulations make contravention of any of the above a criminal offence with a maximum penalty of up to seven years.[11]

2.2.2 Exceptions and Licences

The Global Human Rights Regulations set out a number of exemptions from the offences created (as described in more detail above), such as allowing a frozen account to be credited with interest due or by crediting a frozen account with funds transferred to it.[12]

Alongside these exemptions sit licences issued by HMRC that can authorise specific acts otherwise prohibited under the Global Human Rights Regulations by specifying certain acts. HMRC may also impose conditions on the licences, such as a time frame, or only authorise acts by a particular person. In addition, licences from the Channel Islands, the Isle of Man or any British overseas territory can also authorise certain activities otherwise prohibited under the Global Human Rights Regulations.[13]

2.2.3 Reporting obligations

"Relevant firms" have special reporting obligations under the Global Human Rights Regulations and are defined to include, amongst other, businesses that operate a currency exchange or transmit money, auditors, accountants, lawyers, trusts, businesses that set up companies, estate agents and companies that deal with valuable metals, such as gold.[14]

Organisations designated as a "relevant firm" are obliged to inform HMRC as soon as practicable if it knows of, or suspects, a breach of the sanctions. When reporting to HMRC, the organisation must clearly state what their suspicion, or actual knowledge, is based on and provide any information about the person it holds by which the person can be identified as well as details about the funds or other economic resources it holds for the person.[15]

In addition to reporting obligations imposed on organisations handling assets or economic resources of designated persons, HMRC may request information or the production of documents from a designated person.[16]

2.3 Outlook

Historically, the UK has only imposed unilateral sanctions on very rare occasions. However, the UK Government seems to have passed SAMLA with the intention of positioning itself as a global defender of human rights now that it has left the EU.

Indeed, a policy paper published by the Government states that it "is likely to give particular attention to cases where the relevant jurisdiction's law enforcement authorities have been unable or unwilling to hold those responsible for human rights violations or abuses to account".[17] An explanatory memorandum, accompanying the Global Human Rights Regulations, goes even further and explains that the Government "seeks to champion human rights, good governance and the rule of law" and that the designation of persons involved in human rights abuses is "intended to deter, and provide accountability".[18]

It will be interesting to see how seriously the UK Government will take its role of self-pronounced defender of human rights and what other sanctions will be imposed in the future. In this regard, it is telling that the first sanctions imposed under SAMLA have been described as the "first wave" with "further sanctions expected in the coming months".[19]

3. Commerzbank fine: Lessons to be learnt by all firms

The FCA has signalled its intention to continue to come down hard on firm's breaches of anti-money laundering obligations. The fine of £37.8 million imposed on Commerzbank AG's London branch is a hefty fine with an accompanying strong deterrent message for the market more generally.

3.1 Increased AML enforcement risk

There is an increased risk of enforcement in AML cases. The FCA's 2020/2021 Business Plan notes that it will continue to take enforcement action in financial crime matters where the FCA uncovers serious misconduct "particularly where there is a high risk of money laundering".

In a speech given in April 2019, the FCA's Director of Enforcement, Mark Steward, said that "I think it is time that we gave effect to the full intention of the Money Laundering Regulations which provides for criminal prosecutions". The speech was foreshadowed by the FCA signalling that it intended to pursue more dual-track money laundering investigations, that is, running investigations as both civil and criminal investigations. This raised prospects of an increased risk of criminal prosecution for breaches of procedural AML obligations which might not have facilitated any substantive money laundering.

These matters confirm the risk of enforcement action being taken where the regulator identifies breaches either of its systems and controls (SYSC) requirements or breaches of the Regulations.

The fact that the FCA has imposed a significant fine on Commerzbank for breaches of anti-money laundering (AML) compliance obligations is, therefore, not surprising. The fine is for a very significant amount but it should not be forgotten that the FCA have fined both Deutsche Bank and Standard Chartered Bank over £100 each for AML contraventions.

3.2 Why do firms get it wrong?

One surprising aspect of money laundering enforcement is that Final Notices issued by the FCA invariably cover the same well-trodden ground of breaches of obligations relating to customer due diligence (CDD), high-risk jurisdictions, PEPs and monitoring. In the Commerzbank case the FCA's investigation covered a broad period of time over which breaches were occurring, which the bank's own internal audit team had identified, yet appropriate remediation measures had not been taken sufficiently quickly.

The Money Laundering Regulations set out seemingly clear obligations around the performance of customer due diligence checks, the assessment of risk and the monitor of transactions. In practice, these obligations can be difficult to comply with, particularly for large firms with a large number of clients and transactions and where the business has exposure to multiple jurisdictions. They are operationally difficult to apply and can require considerable human as well technological resources.

A further dynamic is the impact of AML controls on a firm's business. The MLRO might potentially have to veto the onboarding of new clients or the execution of transactions. MLRO might also have to decide to report clients to the NCA or other FIU. This can, of course, create tension with the business.

3.3 FCA action against Commerzbank

In June 2020 the FCA imposed a fine of £37.8 million on Commerzbank AG's London Branch for breaches of the Money Laundering Regulations 2007 (the ML Regulations). The ML Regulations have, of course, been superseded by the Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017 (the 2017 Regulations). However, since the 2017 Regulations contain the same fundamental obligations as the ML Regulations, albeit with a greater focus on a risk-based approach, the Commerzbank base is good learning for firms.

3.4 Dealing with issues promptly

The FCA's action covered a broad period of time from 23 October 2012 to 29 September 2017.

An important feature of the case was that concerns about various different AML compliance issues had existed over a lengthy period of time and had been raised by the bank's own Internal Audit team. A Skilled Person under s.166 of the Financial Services and Markets Act 2000 had also been appointed in 2017.

The FCA was not the first regulator to have concerns about Commerzbank's AML compliance. The New York Department of Financial Services had taken action against Commerzbank's New York branch and an independent monitor had been appointed to review and report on, amongst other things, weaknesses in the banks AML control framework at Commerzbank's London branch.

These are all matters that pointed to the bank needing to take appropriate remedial action.

The manner in which a firm deals with issues once identified, including notifying regulators, remediating processes and controls and addressing any substantive consequences of errors or breaches are all important issues which impact on the regulatory response to failings.

We consider below some of the issues raised in the FCA's Final Notice.

3.4.1 Intermediaries

The bank was criticised by the FCA for failings in relation to the conduct of due diligence on introducers and distributors. The FCA's Final Notices explained that the Private Banking Sales area of the bank dealt directly with customers but some of these were introduced by intermediaries.

A firm needs to consider the nature and extent of its AML controls in circumstances where it does not have direct access to a customer and is instead dealing with the customer through intermediaries such as business introducers.

In addition to the above, intermediaries are a source of ABC (bribery and corruption risk) and risks in relation to intermediaries also need to be assesses for these reasons.

A number of issues arose in relation to intermediaries including the failure by some staff members to comply with instructions provided not to deal with certain intermediaries following a reduction in the intermediaries with whom the bank would deal.

More generally, both the bank and the Skilled Person found that insufficient due diligence was being conducted on intermediaries. In 2016 the bank's Internal Audit identified inconsistencies in policy documentation used by different parts of the bank that produced discrepancies in the due diligence undertaken. There was also a lack of awareness by some parts of the bank of the intermediaries policy.

The Skilled Person found that due diligence on introducers was inadequate and inconsistent. The Skilled Person found that files revealed unidentified red flags, red flags that had been identified and not investigated and a lack of a risk-based approach to due diligence.

These matters all created risks for the bank.

Firms should have processes to identify relationships with intermediaries and assess the risks arising from those relationships both in an AML and an ABC context. Appropriate due diligence should be carried out on intermediaries and this should be reviewed periodically with risks being reassessed.

3.4.2 Politically exposed persons (PEPs)

PEPs are a key area of risk that have featured prominently in other enforcement action taken by the FCA for breaches of AML obligations.

The issue of PEPs was reviewed by the Skilled Person. The Skilled Person found that there were inadequacies in the identification and screening of PEPs.

- No evidence on certain files that PEP and sanctions screening had been undertaken on the customer, its beneficial owners and/or connected parties.
- PEPs were identified as being closely linked to a customer yet there was no evidence that the AML risks posed by the associated individuals were considered.

- Commerzbank was not able to demonstrate that it was conducting ongoing screening for PEPs or customers, meaning that events that ought to trigger a review might not be identified.

The above failings in relation to PEPs were all failings to carry out basic procedures around PEPs appropriately.

PEPs are an area of high risk and close regulatory attention.

Firms should review processes around PEPs. One important aspect of controls around PEPs is to obtain senior management approval to onboarding clients who are PEPs or whose UBOs are PEPs. However, it is also important to apply controls on an ongoing basis and not just at the time of onboarding.

3.4.3 Verifying the beneficial ownership of clients, including high-risk clients, from a reliable and independent source

AML obligations require that firms must take a risk-based approach to determine whether the identity of a beneficial owner can be verified by the customer or by information obtained from a reliable and independent sources. For low-risk customers it may be reasonable for a firm to confirm the beneficial owners identity based on information supplied by the customer.

The Skilled Person found that in 46% of CDD files reviewed the bank had failed to identify and verify the identity of beneficial owners. The Skilled Person attributed this to the fact that Commerzbank was too willing to accept responses and information from the customer without independently verifying or challenging them.

In performing CDD and associated measures the starting point is that the firm should seek verification from sources independent of the client. It is usually difficult for firm's to achieve compliance in reliance on information that the client has itself provided to the firm. In some cases it will be difficult for the firm to obtain information from public registers. In such cases the firm must take a holistic approach and the information a client is able to provide might be one component of this.

3.4.4 Offboarding clients

AML controls focus closely on the client onboarding processes, the information that must be obtained to pass onboarding and the internal approvals that are required. The Commerzbank case highlights the fact that offboarding processes are also important.

In the Commerzbank case, the bank did not generally offboard clients even where their accounts were dormant. This resulted in the risk of transactions taking place on accounts of clients who should have been offboarded. The FCA found that no comprehensive documented process or criteria existed for terminating a relationship with an existing client for financial crime risks. The FCA said that the firm should have had documented criteria for identifying clients that posed too high a financial crime risk so as to better enable the firm to adopt a uniform approach to offboarding clients in line with this financial crime risk appetite.

3.4.5 The Refresh Backlog

Money laundering regulations require firms to refresh customer due diligence obtained on clients. Firms must assess the risks of customers and determine appropriate periods within which refreshes of CDD information are to be carried out. Clearly, refreshes for higher risk customers will need to be carried out more frequently. The corollary of course is that less frequent refreshes as acceptable for lower risk customers.

Determining the appropriate refresh can be challenging but equally, firms must ensure that resources are available to perform refreshes at the relevant times. As stated above already, a lot of focus can be placed on the initial onboarding stage given imperatives to get clients into a firm. However, from a compliance standpoint, the refresh is equally important given that ownership and risks related to particular client can have changed.

In Commerzbank's case a significant backlog built up in refresh files. In other words the firm was not able to process refreshes sufficiently promptly. This gave rise to the risk of the firm continuing to deal with clients where the risks associated with the client had not been appropriately checked and reassessed. The FCA said that the bank had tried to address the CDD/KYC refresh backlog. However, the FCA's view was that the measures taken were too late and effected too slowly.

3.4.6 Transaction monitoring

Transaction monitoring is a key part of an AML control framework but it is notoriously difficult to implement an effective monitoring tool where a firm is seeking to monitor large volumes of transactions.

Regulation 28(11) of the 2017 Regulations provides that firms must conduct ongoing monitoring of a business relationship including scrutiny of transactions to ensure that the transactions are consistent with the relevant person's knowledge of the customer, the customer's business and risk profile.

In its Final Notice the FCA states that as part of its obligation to monitor all business relationships with existing clients a firm must also scrutinise customer transactions to ensure that they are consistent with the firm's knowledge of the customer, its business and its risk profile. Where the business relationship is considered to be high risk this monitoring must be more frequent or more intensive.

The FCA's Final Notice stated that Commerzbank London's automated tool for monitoring money laundering risk on transactions for clients "was not fit for purpose", and did not have access to key information from certain of Commerzbank's transaction systems. The appropriate information was not being fed into the tool, including for example the fact that that tool did not incorporate risks relating to 40 high risk jurisdictions. Given the deficiencies in the monitoring tool the firm was not in a position to demonstrate that it was appropriately monitoring AML risk on an ongoing basis.

3.4.7 Governance

Finally, and importantly, from a governance perspective, the FCA found that risk and issue owners were not clearly articulated or understood by Commerzbank London's committees. This led to a "lack of clarity around responsibilities", which impacted the Front Office and Compliance.

In the SMCR world all firms must ensure appropriate allocation of roles and responsibility for them. Individuals are under greater scrutiny to ensure that they understand their roles, the risks for which they are responsible and that they discharge their duties responsibly.

4. UK courts review the scope of Unexplained Wealth Orders

Unexplained Wealth Orders (UWO) are a relatively recent phenomenon. They are certainly a potentially useful tool for law enforcement but of very broad application and prejudicial effect to those who find themselves the subject of such orders. It is these conflicting strains that have recently produced Court judgments, which have both upheld and resulted in the discharge of UWOs in different cases. Given their potentially draconian effect, it is clear that the Courts will insist on proper evidence being submitted if UWOs are to be upheld.

4.1 UWOs

UWOs came into force in January 2018 after the Criminal Finances Act 2017 had expanded the legislative scheme for the recovery of criminal assets laid down in the Proceeds of Crime Act 2002 to enhance the UK law enforcement response to unexplained wealth and improve its capability to recover the proceeds of crime.

The order is described as relating to "unexplained wealth" given that it bites on property which the subject of the order does not have the means to acquire. This discrepancy between the value of property owned and the subject's income suggests that the property has been acquired through illicit means.

4.1.1 Criteria

UWOs are designed to confiscate the proceeds of crime by using civil powers; they are a means of obtaining information against persons and property about whom little information is available. Any of NCA, HMRC, FCA, SFO, or DPP[20] can apply for a UWO to a High Court judge. An order can be granted on a 'without notice' basis, meaning that person who is the subject of the order will not be given notice of the Court hearing and will find out about the order only after it has been obtained.[21] Before granting a UWO, the Court must be satisfied that:

- there is reasonable cause to believe that the subject of the order holds the property, and the value of the property is greater than £50,000;
- there are reasonable grounds for suspecting that the known sources of the respondent's lawfully obtained income would have been insufficient for the purposes of enabling the respondent to obtain the property; and
- the respondent is a politically exposed person or that there are reasonable grounds for suspecting that the respondent is, or has been, involved in serious crime (whether in the UK or elsewhere), or is a person connected with the respondent who is, or has been, so involved.[22]

Taking each of the above criteria in turn, the person (which includes a body corporate) and property must be specified, but either or both may be located outside the UK.[23] "Holding" a property means: (i) having effective control over it; (ii) being a trustee of a settlement in which the property is compromised; or (iii) being a beneficiary (actual or potential) in relation to the settlement. Whilst the legislation is silent on the type of evidence required to support the alleged disproportionality between lawful income and the property, it is clear that income will be lawful if lawfully obtained under the laws of the country from where it arises[24] and that it is to be assumed that the property was acquired for a price equivalent to market value.[25] Finally, the respondent either has to be a politically exposed person (PEP)[26] or there must be reasonable grounds to suspect that they are involved in serious crime[27] or are connected[28] to a person who is. This means that if the respondent is a PEP, there is no need for any suspicion of criminality.

Interestingly, there is no public interest consideration and the High Court maintains a discretion whether or not to grant a UWO, even if all the constituent elements are made out.

In practice, a UWO will often be combined[29] with an interim freezing order (IFO) to avoid the risk of any recovery order being frustrated.

4.1.2 Responding to a UWO

A UWO compels a person (the respondent) to explain the provenance of specific property within a set time frame to the enforcement authority. The respondent has to provide a statement:

- setting out the nature / extent of the respondent's interest in the property;
- explaining how the respondent obtained the property (including how any costs incurred in obtaining it were met);
- where the property is held by the trustees of a settlement, the details of the settlement as specified; and
- any other such information in connection with the property, as may be specified.[30]

It is important to note that a UWO has effect in spite of any restriction of the disclosure of information however imposed,[31] but legal privilege is preserved. Whilst the legislation contemplates that the provided information may be used in other proceedings,[32] it may not be used against the respondent in criminal proceedings, but there is no prohibition on it being used to further a criminal investigation.[33]

4.1.3 Consequences of a UWO

It is not a criminal offence to fail to comply, unless the respondent makes a deliberately misleading or false statement.[34] Non-compliance without a "reasonable excuse" means that the recoverability presumption arises.[35]

If an explanation is provided and an IFO is in force, the enforcement authority has 60 days to decide whether to commence recovery proceedings or to discharge the IFO if no action is taken.36 If a UWO is not accompanied by an IFO, no time limit applies.[37]

4.2 The "Harrods" Case

The first ever UWO was granted without notice in February 2018 against Mrs Hajiyeva, who is the wife of the former chairman of the International Bank of Azerbaijan in which the State of Azerbaijan had a controlling stake. He is serving a 15-year prison sentence for fraud and embezzlement and Mrs Hajiyeva is also wanted by Azerbaijani authorities, but managed to fight extradition.

During the period that her husband had been chairman, a Knightsbridge home worth £11.5m had been purchased through a BVI company and Mrs Hajiyeva infamously spent approx. £16m in Harrods.

On her 2015 UK visa application, Mrs Hajiyeva declared she was the beneficial owner of the BVI company. In support of the disproportionality between the lawful income and the Knightsbridge home, the NCA relied on evidence of Mr Hajiyev's salary, the rate at which the mortgage was repaid and Mr Hajiyev's fraud convictions.

4.2.1 Challenging the UWO

Mrs Hajiyeva unsuccessfully sought to discharge the UWO arguing that: (i) she was not a PEP; (ii) that her husband's convictions could not safely be relied upon due to Azerbaijan's poor human rights record; (iii) that answering the UWO would self-incriminate; and (iv) that disclosure of information would likely lead to an infringement of her and her husband's human rights.

In March 2019, leave to appeal was granted on the basis that it was the first UWO to come before the courts and further guidance would be beneficial. Appeal was based on several grounds with the most important set out below:

- The interpretation of what constitutes a PEP: Mrs Hajiyeva argued that that there was a distinction between someone only carrying out a public function in relation to a state-owned enterprise, and someone having been "entrusted" with such public function. The Court rejected this argument on the basis that the focus is on the status of the person, not how they had come to gain it.
- The UWO offended the rule against self-incrimination and spousal privilege: Mrs Hajiyeva tried to argue that providing an explanation to the UWO would incriminate herself and her husband, but the Court rejected this argument due to the statutory prohibition to use information obtained from a UWO in a criminal proceeding.[38]

In addition, Mrs Hajiyeva had sought to argue that the bank was not a "state-owned enterprise" and that the "income requirement" had not been met. The Court similarly dismissed both those grounds as well and clarified that the application of the provisions will ultimately be a question of English law.

4.3 One step forward, two steps back for UWOs?

Following the Court of Appeal decision in February this year, it seemed that judicial guidance had opened the door to more UWOs as the Court interpreted the statutory regime widely, placing the burden of proof firmly on the respondent. However, in April, the High Court discharged three UWOs relating to two Kazakh individuals and a property in Kensington.

Discharging the UWO, the Court held that the requirements for making a UWO had not been met and that beneficial ownership and funding of the properties was no longer "unexplained". In a harsh assessment of the NCA's case, the Court held the NCA's evidence "unreliable" and dismissed the argument that the use of complex corporate vehicles and structuring in offshore locations was in itself suspicious and proof that funds were being sued for wrongful purposes.

The NCA is now appealing, but this judgment certainly strikes a blow to the enforcement agency, which had appeared to gear up to using UWOs more frequently. Indeed, in 2019, the NCA disclosed that it had considered 140 matters for UWO suitability. Whether these applications will now be made, may well depend on the appeal ruling.

5. The new regulator on the block: How fining Standard Charter Bank (SCB) put the Office of Financial Sanctions Implementation (OFSI) on the map of the sanctions enforcement landscape

Earlier this year, the OFSI imposed a penalty of £20.4 million on SCB for breaches of financial sanctions pursuant to Pt 8 of the Policing and Crime Act 2017; the largest fine since the establishment of the OFSI in 2016. Whilst it remains to be seen whether the size of the monetary penalty was an outlier or an indication of things to come, the imposition of such a fine seems to have established the OFSI as a noteworthy force.

5.1 The OFSI

The OFSI was established as a statutory body to administer and enforce economic sanctions by the UK government in 2016, and granted the authority to impose financial penalties on those breaching such sanctions in 2017. Penalties may be imposed on a person (which includes legal persons) that:

- breached a prohibition, or failed to comply with an obligation, imposed under financial sanctions legislation; and
- such person knew, or had reasonable cause to suspect, that they were in breach of the prohibition or had failed to comply with the obligation.[39]

Pursuant to s.146 of the Policing and Crime Act 2017, the OFSI may impose maximum penalties of £1 million or 50% of the estimated value of the funds or resources involved, whichever is the greater.[40] Interestingly, it seems that fines can be imposed on a per breach basis.[41]

It is worth noting that every case that has been determined to be in breach of financial sanctions by the OFSI is considered "serious", but some are considered the "most serious", for example if they involve a very high value, create lasting damage or involve an obvious flouting of the law.[42]

Prior to the SCB fine, the OFSI had only used its powers sparingly and imposed three rather small fines ranging from £5,000–£146,000.[43]

5.2 The background

Following the annexation of Crimea in 2014, the EU adopted the following regulations to impose sanctions against certain Russian companies and non-EU companies which are owned to 50% or more by the targeted companies. Article 5(3) of EU Council Regulation 833/2014 (the Regulation) and reg.3B of The Ukraine (European Union Financial Sanctions) (No.3) Regulations 2014 prohibit EU persons from making loans or credit of a maturity of over 30 days, or being part of an arrangement to make loans or credit, available to sanctioned entities. However, art.5(3)(a) of the Regulation provides an exemption which permits loans or credits that have the purpose of financing the import or export of non-prohibited goods between the EU and any third country (the article 5(3) exemption).

One of the companies targeted by these so-called "sectoral sanctions" was Sberbank. Prior to the sanctions coming into force, SCB had a relationship with Denizbank, a Turkish private bank in which Sberbank held the majority stake. Whilst SCB appeared to have ceased the relationship in 2014, it resumed making loans available to Denizbank in 2015, seemingly relying on the art.5(3) exemption.

From 2015 to 2018, SCB made a total of 102 loans available to Denizbank until SCB self-reported its violation of the Regulation to the OFSI in 2018. The OFSI investigated and ultimately concluded that of the 102 loans, 70 loans were in fact in breach of the Regulation and not covered by the art.5(3) exemption. However, as the OFSI's enforcement powers only permitted it to impose penalties for violations that occurred after April 2017 only 21 loans, worth about £97.4million, were in scope. The OFSI ultimately imposed two penalties on SCB in August and December 2019 totalling £31.5million.

SCB elected to have the penalty reviewed by a Minister of the Crown of the Treasury (the Treasury Minister),[44] who upheld the finding that SCB violated the sanctions imposed by the Regulation, but reduced the penalty from £31.5million to £20.47 million. The penalty was reduced because it was found that SCB: (i) had acted in good faith and had not purposefully breached the Regulation; and (ii) had self-reported and fully cooperated with the OFSI, including taking remedial actions.

5.3 Key learning takeaways

5.3.1 Being compliant requires more than mere good faith

Both the OFSI and the Treasury Minister on review found that SCB had acted in good faith, yet nevertheless determined the breach to be a "most serious case". It is vital that financial institutions and companies impacted by the sanctions understand that good faith is insufficient to prevent a penalty for any breaches.

5.3.2 The need for robust compliance measures

SCB had initially ceased trading with Denizbank when the sanctions were put in place, but later commenced trading again using the article 5(3) exemption. Effective implementation of restrictive sanctions requires more than just literal adherence to the law. Instead, it is critical that financial institutions and companies carry out robust checks and bespoke risk assessments as well as ongoing monitoring to ensure compliance. Whilst the OFSI does not mandate a particular standard of compliance, it recommends that it is good practice to continuously review the relevant processes.[45]

5.3.3 Increase in size of penalties

The SCB penalty represents a harsh increase in the value of penalties imposed by the OFSI, with the previous penalties only ranging from £5,000–£146,000 (originally £300,000 but reduced on review). Whilst it is too early to predict the size of any future penalties, the size of the SCB penalty established the OFSI as a noteworthy sanctions force.

5.3.4 Self-reporting reduced the penalty by 30%

The OFSI values voluntary disclosure. SCB's self-reporting led to the maximum reduction of 30% of the penalty in line with the OFSI guidance for the "most serious cases". In cases that are considered "serious", the OFSI will make up to a 50% reduction for prompt and voluntary self-disclosure.[46]

5.3.5 The benefit of review

SCB's penalty was reduced by £11.03million on review as the Treasury Minister concluded that the OFSI had not given adequate weight to mitigating factors when calculating the fine. It is notable that SCB was not the first to successfully use the review procedure as Telia's penalty in 2019 was reduced by over 50%.

6. Zero Tolerance: The European Union's AML and CTF Action Plan

The European Union has launched an ambitious Action Plan tasked with improving standards and co-ordination of AML and CTF efforts across the EU. It is built on six pillars, which we run through below. The Action Plan was launched on 7 May 2020 and is formally entitled the "Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorism Financing".

Of course, with the UK leaving the EU, the extent to which the Action Plan will be relevant to the UK remains to be seen. However, at a general level we will all need to remain interested in the developments in continental Europe given that these will undoubtedly influence UK developments and, moreover, many businesses operate across Europe which will bring them within scope to some extent at least.

The European Commission states that the Action Plan is aimed at improving the EU's overall fight against money laundering and terrorist financing, as well as strengthening the EU's global role in this area. Combined, the six pillars of the Action Plan are intended to ensure that EU rules are more harmonised and more effective. The Commission also wants the rules to be better supervised and coordinated between Member States. The EU adopted its First Money Laundering Directive back in 1990. The Directives have been minimum harmonisation directives meaning that Member States have not been required to implement the directives in a fully harmonised manner. There are material differences in local implementing laws. In addition to this, recent scandals have shown that supervision of compliance with AML and CTF laws varies tremendously across the EU. Weak links in the chain have been exposed which create the opportunity for money launderers to place money into the European financial system.

The Six Pillars	Summary
1. Effective application of EU rules	Inconsistencies across the EU; "weak links in the chain"
2. Single EU Rulebook	There are variations in the way Member States have implemented ML Directives. In contrast to other areas law are more fragmented. The Commission wants to move to a Single Rulebook. New rules are expected in Q1 of 2021.
3. EU level supervision	Role for the European Banking Authority as the EU level AML/CTF supervisor
4. FIUs: co-ordination and support	The Commission proposes establishing an EU mechanism to help further coordinate and support the work FIUs. The proposals are to be issued in Q1 of 2021.
5. EU level criminal law and information exchange	Better judicial and police co-operation across the EU and sharing information with the private sector
6. EU's global role	EU intends to take a more consolidated approach as a single entity on the global stage. The EU has issued a new list of high risk third countries.

We review the six pillars of the Action Plan below.

6.1 Effective application of EU rules

As noted above, a major weakness of the current system is that the existing body of European AML and CTF laws is not properly implemented, supervised or enforced. Therefore, as a starting point at least, it is a case of ensuring the existing laws are implemented, properly supervised and enforced. The Commission states that it will continue to monitor closely the implementation of EU rules by Member States to ensure that national rules are in line with the highest possible standards.

The Fourth Money Laundering Directive was required to be implemented in June 2017. In fact, the Commission was required to launch infringement proceedings against all Member States for a failure to properly transpose the requirements of the Directive. Some Member States have still not properly implemented new laws to give effect to the Directive even by 2020 (some three years late). For example, in 2020 the Commission announced that it had sent a letter of formal notice to Estonia on the grounds that it had incorrectly transposed the Fourth Money Laundering Directive. The Commission stated that it has concluded that Estonia has not correctly transposed the Directive in respect of the treatment of politically exposed persons, beneficial owners, the performance of risk assessments and risk management systems, and access rights of the Financial Intelligence Units (FIUs) to information.

Problems with effective transposition have continued with the Fifth Money Laundering Directive. This was required to be transposed into national laws by 10 January 2020. In February 2020 the Commission sent letters of formal notice to Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia, and Spain for not having notified any implementation measures for the Fifth Money Laundering Directive.

An important part of efforts to ensure consistency will involve the new role of the planned Pan-European AML regulator (likely the European Banking Authority), which we comment on below.

6.2 A single EU rulebook

The Money Laundering Directives are "minimum harmonisation" directives. This can be contrasted with the direction of travel of banking and financial services regulations which are now highly detailed and co-ordinated across the EU. Not only are the single market directives in this area "maximum harmonisation" (i.e., they have to be implemented strictly in accordance with the directive so that most Member States take a copy out approach), the EU has made use of Regulations (which do not need to be transposed into local law) and delegated legislation, whereby the Commission has been conferred with the authority to issue EU level laws which are usually prepared by one of the European Supervisory Authorities such as the EBA. This massively co-ordinated approach has produced a level playing field of laws across the EU for the regulation of banking, financial services and insurance. Of course, this approach has also come at the cost of a 'one size fits all' approach and removal of national discretion as to how these issues are approached.

The Commission states that while current EU rules are far-reaching and effective, Member States tend to apply them in a wide variety of different manners. The Commission has acknowledged that diverging interpretations of the rules lead to loopholes, which can be exploited by criminals and states that EU legislation "needs to become more granular, more precise and less subject to diverging implementations".

The Commission proposes converting AML/CTF requirements into directly applicable regulations. In order to address these concerns the Commission is proposing a more harmonised set of rules for Q1 of 2021.

6.3 EU-level supervision

Member States are presently responsible for supervision of AML compliance by Obliged Entities (i.e., firms who are within the regulated sector for AML purposes).

The lack of an EU level supervisor has been recognised already and the mandate of the European Banking Authority (EBA) was enhanced in 2019 pursuant to the Regulation 2019/2175 of the Parliament and Council. The effect of this Regulation, which came into force in January 2020, was to consolidate into the EBA all of the AML supervisory responsibilities of the European Supervisory Authorities, that is the EBA as well as ESMA and EIOPA.

The Regulation also gave the EBA a clear legal duty to contribute to preventing the use of the financial sector for the purposes of money laundering and terrorist financing, as well as to lead, co-ordinate and monitor AML and CTF efforts of all EU financial services providers and Competent Authorities. In this role the EBA has been reviewing the approach of regulators in Member States and published its first report on the EBA's implementation reviews in February of this year. In this report the EBA has observed that local regulators' supervision of AML/CTF compliance by banks was "not always effective". This conclusion is hardly surprising given the major money laundering scandals that have afflicted banks in the EU.

In spite of the EBA's enhanced mandate, the Commission notes that currently it is still up to each Member State to individually supervise EU rules in this area and as a result, gaps can develop in how the rules are supervised.

The Action Plan contains proposals for the EU regulator to have:

- direct AML/CTF supervisory powers over certain regulated sector firms (obliged entities);
- clear powers to oversee and instruct national authorities to carry out AML/CTF related tasks; and
- enhance co-ordination with supervisors outside the EU.

It is clear that the Commission envisages that the EU level regulator will take a hands-on approach to supervision. The Commission states that the regulator will have the ability to review internal policies, procedures and controls as well as their effective implementation. In addition, it will have power to review documentation on transactions and customers. The EU level regulator might also be entrusted with enforcement of EU financial sanctions.

As an alternative, the Commission has proposed that the EU level regulator would carry out its tasks in co-ordination with the local regulators.

The Action Plan contains discussion over whether the EBA should take over the role of the EU regulator or whether this should be entrusted to a new body. From a practical perspective, it would seem sensible to entrust this role to the EBA, which could assume its extended powers more quickly and at a lower cost.

Establishing a new regulator would, on the other hand, be attractive given that the regulated sector already contains non-financial businesses such as gaming, which do not fit neatly into the financial sector regulatory construct and the role of the EBA as a banking regulator.

6.4 A coordination and support mechanism for Member State Financial Intelligence Units

The Commission acknowledges the role played by Financial Intelligence Units (FIUs) in Member States. The Commission states that FIUs play a critical role in identifying transactions and activities that can be linked to criminal activities.

The Commission notes in the Action Plan that there are presently weaknesses with respect to how FIUs apply the rules and co-operate between themselves and with other authorities at a domestic level and across the EU. It is for this reason that the Commission proposes that an FIU co-ordination and support mechanism should be established at the EU level with a view to addressing these weaknesses. The EU level mechanism would, amongst other things:

- identify suspicious transaction with a cross-border element;
- perform joint analysis of cross-border cases;
- identify trends and factors relevant to assessing the risk of money laundering and terrorist financing at a national and supranational level;
- enhance co-operation amongst competent authorities; and
- adopt or propose standards or measure for the functioning of FIUs under the new integrated Single Rulebook.

Proposals for the above are intended to be issued in Q1 of 2021.

6.5 Enforcing EU-level criminal law provisions and information exchange

The Action Plan provides an overview of the steps taken to co-ordinate approaches at the EU level to criminal enforcement. This section of the Action Plan does not formulate new proposals as such, buts the developments across a range of relevant areas.

One development that is mentioned is the Sixth Money Laundering Directive, which is required to be implemented in Member States by 3 December 2020. The purpose of the Directive is to co-ordinate the approach across the EU to criminal money laundering offences. EU criminal law provisions do not apply automatically to the UK which is required to opt into the relevant legal provisions. The UK Government has not opted into the Directive on the basis that it considers that UK law already implements most of the requirements. Most importantly from a co-ordination perspective, the Directive specifies 22 offences that are required to be treated as predicate offences for money laundering purposes so that there is consistency of approach to the definition of money laundering in Member States.

The Action Plan sets out the desire to build capacity at the EU level to investigate and prosecute financial crime. In this connection it notes that Europol has stepped up efforts in order to tackle economic and financial crime with the new European Economic Crimes Centre (EECC), which is intended to become operational later this year. The EECC will concentrate all financial intelligence and economic crime capabilities in a single entity within Europol. The Commission further notes that the European Public Prosecutor's Office is due to take up operations at the end of 2020 and will be competent to investigate and prosecute money laundering offences linked to crimes against the EU budget. It notes that judicial and police co-operation, on the basis of EU instruments and institutional arrangements, is essential to ensure the proper exchange of information.

6.6 The EU's global role

The EU intends to focus on ensuring that its Member States speak with a single voice on money laundering issues. The Commission states in the Action Plan that "We are determined to step up our efforts so that we are a single global actor in this area".

The EU has already formalised its role in connection with Third Countries. The Fourth Money Laundering Directive sets out in art.9 a Policy on High Risk Third Countries. The Action Plan notes that, in particular, the EU will need to adjust its approach to third countries with deficiencies in their regime regarding anti-money laundering and countering terrorist financing that put the Single Market at risk.

The publication of the Action Plan was accompanied by the new list of High Risk Third Countries. Preparation of the list was controversial with the Commission taking a more expansive approach than the Council, originally proposing that Saudi Arabia certain US territories.

The Action Plan contains a large number of interesting and transformational proposals that stakeholders should engage with. The Commission has launched a public consultation which is open for feedback until 29 July 2020.

7. Human Rights Diligence Catching Up To Anti-Corruption

An April 29 announcement from Didier Reynders, the Commissioner for Justice of the EU may be the final step in elevating human rights due diligence to a business imperative, akin to anti-corruption diligence. Human rights diligence has been gaining steady momentum over the past several years, moved by many of the forces that propel anti-corruption diligence. These include national laws, civil and criminal legal risks, the wish to protect employees, access to financing and capital, and benefits operationally. The missing ingredient—perhaps the most important one—has been a broad legal requirement coupled with an enforcement mechanism that is similar to the anti-corruption framework that exists worldwide. The EU Commissioner's pronouncement, building on domestic legal efforts across the continent, may provide that ingredient. According to Mr. Reynders, in early 2021, the Commission will present a legislative initiative compelling diligence throughout companies and their supply chains, with accompanying enforcement and civil liability provisions. This Article discusses how the dynamics that propelled anti-corruption diligence to become engrained in business activities have been growing in the human rights due context, and the significance of a compulsory regime throughout Europe in pushing human rights diligence to a similar level.

7.1 Anti-Corruption Diligence

Over the past 15 years, anti-corruption due diligence has become a core aspect of global business activities. While the US Congress enacted the Foreign Corrupt Practices Act (FCPA) in 1977, it was only after the OECD adopted the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions in 1997, and the UN Convention Against Corruption became effective in 2005,[47] that anti-corruption diligence began to grow in line with a dramatic shift in enforcement priorities. In 2006, there were some 14 FCPA enforcement actions. That jumped sharply in 2007, as the US Department of Justice (DOJ) initiated 22 enforcement actions, and the Securities and Exchange Commission (SEC) initiated 21, starting an aggressive enforcement regime that continues to grow. In 2019, DOJ pursued 32 actions and the SEC 17, and $2.9 billion was collected in corporate settlements, the largest total to date.

Consistent with the OECD Convention, DOJ and the SEC interpret the FCPA to require that companies pursue anti-corruption diligence in multiple contexts. These include: third-party diligence, especially government intermediaries or third parties affiliated with the government or government officials; diligence of prospective employees to assess whether they are PEPs (politically exposed persons); risk assessments, program testing and other types of program diligence; and diligence during investments, mergers and acquisitions, and transactions. Dozens of enforcement actions, including jail time for individuals and massive fines and penalties for companies, have resulted from the failure to conduct diligence when there are known "red flags" that suggest bribery could be afoot.[48] Across the pond, the UK Serious Fraud Office (SFO) and other European law enforcement authorities also have increased their enforcement efforts, and TRACE International's annual Global Enforcement Report provides that authorities in 37 countries had open corruption investigations at the end of 2019.[49]

While the active enforcement of domestic corruption laws has been a key driver for anti-corruption diligence, anti-corruption diligence has now become entrenched in a much larger legal and business framework. For example, corruption allegations have become a frequent defense by governments in the investor-state arbitration context.[50] Similarly, multi-national businesses widely recognize the fundamental responsibility to keep employees safe, as the COVID-19 crisis has underscored, and accusations of corruption bring dramatic risks to the welfare of local personnel; in fact, we have seen many instances in the recent past where developing countries have manufactured corruption claims against individuals to pressure their employers.[51] It is also now routine for financial institutions and investors to pursue details on corruption programs, risks and specific issues as part of their diligence exercises, making a weak corruption approach a threat to access to capital.[52] The same is true in the M&A context, even in locales with lower risks of corruption, and thus where enforcement risks are not immediately evident. More and more governments and their development agencies also are conditioning diplomatic and export credit support on anti-corruption commitments and performance. Similarly, public procurements be they local, national, or international commonly contain anti-corruption/integrity rules.[53]

As these dynamics show, while enforcement risk was the spark that ignited the flame of anti-corruption diligence, and remains an important reason it is pursued, it is no longer the only reason. In fact, anti-corruption diligence has become assimilated into global business operations to a degree that should DOJ, the SEC, SFO, and other enforcement efforts were somehow to slow, anti-corruption diligence likely would continue unabated.

7.2 Human Rights Diligence

On a conceptual level, the steps associated with human rights and anti-corruption diligence differ. Unlike anti-corruption, the goal of human rights diligence is not to assess risks to the business, be they financial, reputational, or otherwise. It is also broader than just ascertaining actual, potential, or even perceived risks of negative human rights impact on stakeholders. Human rights diligence is in fact more accurately described as a continuous process of identifying and addressing adverse human rights impacts that may be connected to the business through its activities and relationships. It consists of four principles: (1) determining actual, potential and perceived risks of negative human rights impacts on stakeholders,

including the likelihood, scale, scope, and irremediability of those impacts; (2) taking steps to prevent and mitigate those impacts; (3) evaluating the effectiveness of those steps; and (4) reporting externally, including to potentially affected individuals and groups.[54]

Although there are concrete distinctions between human rights and anti-corruption diligence, many of the same dynamics that have driven anti-corruption diligence are present in the human rights sphere. For instance, human rights abuses bring tangible domestic criminal and civil litigation risks. Domestic criminal laws often prohibit the acts that underlie human rights violations; torture is prosecuted as assault and battery, extrajudicial killings as murder, and enforced disappearance or arbitrary detention as kidnapping. Human rights abuses also are litigated in high-profile transnational tort lawsuits in a swath of home jurisdictions, including the US, Canada, the UK, and elsewhere, and have led to meaningful damage awards and settlements.[55] Likewise, as with anti-corruption, claims of human rights abuse are raised in the international arbitration context, in support of claims and counterclaims, as well as such affirmative defenses as unclean hands.[56] As with anti-corruption, human rights due diligence thus has been undertaken to help companies reduce the likelihood of these legal risks to the company and their employees, and in the mergers and acquisitions context, to avoid inheriting a host of challenging legal and operational risks.

Further, much like the anti-corruption context, investors and lenders are seeking information on human rights and other ESG-issues for lending and financing decisions. The U.S. Financial Crimes Enforcement Network (FINCen) has issued a detailed advisory for financial institutions listing red flags to assist in identifying suspicious financial activity potentially related to human trafficking,[57] and now includes on its Suspicious Activity Report (SAR) form a box to check whether potential suspicious activity may exist. The Financial Action Task Force has promulgated a lengthy report listing human trafficking risks and their connection to financial institutions.[58] Industry efforts also have deepened after the Australian government charged Westpac Bank with a staggering 23 million financial crimes and breaches, some of which facilitated transactions that enabled child exploitation in the Philippines. The CEO was fired, the bank faced a major stock drop, and it is facing potentially $1 billion in fines, and civil and criminal penalties.[59] Financial institutions, such as the 92 members of the Equator Principles Association, which include major banks and export credit institutions, also are increasingly insisting that companies conduct assessments of environmental and social risks before granting financing. The latest version of the Equator Principles framework, EP4, which will go into effect this year, demands that projects assess adverse human rights impacts.[60] Access to capital, and potential regulatory actions, thus have been important in boosting human rights diligence.

Also similar to anti-corruption, governments increasingly are conditioning overseas support to companies, bilateral aid, and public procurement on human rights considerations. For the last several years, U.S. assistance to the governments of El Salvador, Guatemala, and Honduras has been conditioned on protection of human rights, among other concerns.[61] In the corporate context, Canada conditions overseas governmental assistance and economic diplomacy on responsible human rights performance.[62] Recently, the U.K. Government—which spends roughly £50 billion buying goods and services—issued a Modern Slavery Act Statement recognizing that the government is introducing "strong incentives" for suppliers to improve their human rights performance, and issuing a clear warning that suppliers whose human rights performance falls short may face an increased likelihood of being excluded from public contracts.[63] The same is true in Australia, as the government will issue its own Modern Slavery Act Statement later this year, which it believes will "help mitigate modern slavery risks in public procurement and investments".[64]These governmental incentives and initiatives also have contributed to the growing prominence of human rights diligence.

In addition, perhaps even more than with anti-corruption, human rights violations can have profound business risks. In the US, the law prohibits importing goods produced in whole or part by forced labor, and the U.S. Customs and Border Patrol has been increasing its use of Withhold Release Orders (WROs), seizing goods when it receives information that forced labor may have been involved in their

creation.[65] There also have been numerous instances of boycotts, blockades, and business interruptions stemming from poor human rights performance, as a loss of social license to operate can be a death knell for an operation. One well-known study, focusing on the extractive sector, determined that the costs of shutting down operations for a major mining project are roughly US$20 million per week, not to mention the potentially lasting impacts on individuals and communities that human rights violations can bring.[66] The study cited numerous discrete examples reflecting the enormous costs associated with social conflicts, including one operation where community-related delays led to US$750 million in project costs. Companies have recognized that human rights diligence can help avoid these kinds of operational difficulties. On the flip side, as the COVID-19 crisis has underscored, companies with strong due diligence systems tend to have greater resilience, and are better poised for a recovery.[67]

7.3 Mandatory Diligence

Finally, while all of these dynamics have been important in elevating corporate human rights diligence, there have been increasing calls to mandate it. Even before the COVID-19 crisis, many observers were predicting that mandatory human rights due diligence laws—requiring companies to identify, mitigate and report on salient human rights risks—would sweep Europe.[68] Mandatory diligence laws already exist in France and the Netherlands.[69] They have been formally proposed in Norway, Austria, Denmark, and Switzerland. Government leaders in Belgium, Finland, Germany, Luxembourg, and elsewhere have stated that they would support mandatory diligence laws. Scores of major European companies, including more than 50 from Germany and 29 from the Netherlands, as well as more than 100 investors, have likewise voiced their support for mandatory human rights diligence laws.[70]

As part of this clear momentum, earlier this year the EU published a lengthy study on regulatory options for due diligence legislation at an EU level.[71] While the study found support among leading European nations, the announcement this week from Commissioner Reynders may be the final step to advancing human rights diligence to the status of anti-corruption diligence. Commissioner Reynders stated that "voluntary action to address human rights violations, corporate climate and environmental harm … has not brought about the necessary behavioural change", and that only 30% of "businesses in the EU are currently undertaking due diligence which takes into account all human rights and environmental impacts". Consistent with the forces motivating human rights diligence today, he noted that "70% of business survey respondents agreed that EU-level rules on a general due diligence requirement may provide benefits for business," as they will bring "legal certainty and a single harmonized standard" across the EU and sectors. He further announced that he will next year introduce mandatory due diligence legislation as part of the Commission's 2021 work plan, stating that the Commission will launch "public consultation" on the initiative in the coming weeks and table a proposal in the first quarter of 2021. Although he remained general in discussing the components of the requirement, and will include substantial input from the EU Trade Commissioner and others,[72] he stated:

- that the legislative objective will be to require that companies take affirmative steps to identify, prevent, mitigate, and account for human rights risks and impacts, including environmental matters;
- that, much like the French law, the EU law would apply to activities of companies and their subsidiaries, and extend through a company's supply chains;
- the EU rule would require due diligence into potential and actual negative human rights impacts, and public reporting of the results of those efforts and how impacts are being addressed; and
- even more than the French law, the EU requirement would include strong enforcement mechanisms, as "a regulation without sanctions is not a regulation," and access to remedy for victims through civil liability.

The German government immediately expressed its backing for the law, and there is little doubt that further governmental support will follow.

While the French Duty of Vigilance Law may be a starting point for a discussion, numerous obvious and important questions ultimately remain for an EU-wide requirement, which no doubt will be explored in-depth during consultations. That includes the standard of "diligence" that will be required, its jurisdictional reach to companies engaging in commercial activities in the EU but domiciled abroad, and what kind of enforcement and/or remedy mechanisms may be included. Depending on the answers to these questions, it may be possible to pursue integrated human rights and anti-corruption diligence, leveraging efficiencies in risk areas that often are contributing factors to the other.

Regardless, such a law—broadly mandating human rights diligence for companies domiciled or doing substantial business in Europe, their subsidiaries, and their supply chains—may be the needed step in driving human rights diligence to the business imperative of anti-corruption diligence. Although many of the other dynamics that have motivated anti-corruption diligence exist in the human rights context, and human rights diligence increasingly has become integrated into legal and business operations, a far-reaching mandatory law has been lacking. However, even if a common EU approach fails to come to fruition, the vast support for mandatory diligence throughout the European governmental, business, and civil society communities almost certainly will lead to domestic legislation that has the same effect.

7.4 Conclusion

Anti-corruption diligence has become integrated into legal and business operations. While many of its driving forces have pushed human rights diligence to the fore, the primary distinction has been the kind of broad legal mandate that exists in a number of domestic legislations and the related enforcement efforts. That is about to change, whether at an EU level, or among its 27 countries. And lingering in the background, even beyond the EU, is a proposed UN Business and Human Rights Treaty that includes mandatory human rights diligence, driven by an intergovernmental working group that is set to hold its 6th session in the Fall. Human rights diligence is upon us, and it will be important to prepare.

Endnotes

1 See oral statement given to Parliament by the Foreign Secretary on 6 July 2020: *https://www.gov.uk/government/speeches/statement-on-the-global-human-rights-sanctions-regime*.
2 See SAMLA s.1.
3 SAMLA s.41.
4 See Global Human Rights Regulations reg.4.
5 See SAMLA ss.2–8 for more detail.
6 Statement made by Foreign Secretary and Secretary of State, Dominic Raab, on 6 July 2020: *https://twitter.com/DominicRaab/status/1280095228893040642*.
7 For a full list, see *https://www.gov.uk/government/news/uk-announces-first-sanctions-under-new-global-human-rights-regime*.
8 Global Human Rights Regulations regs 11–15.
9 Global Human Rights Regulations reg.16.
10 Global Human Rights Regulations reg.33.
11 Global Human Rights Regulations reg.32.
12 Global Human Rights Regulations reg.18.
13 Global Human Rights Regulations regs 20–21.
14 For the full list, please see Global Human Rights Regulations reg.26.
15 Global Human Rights Regulations reg.25.
16 Global Human Rights Regulations regs 27–28.
17 See *https://www.gov.uk/government/publications/global-human-rights-sanctions-factors-in-designating-people-involved-in-human-rights-violations/global-human-rights-sanctions-consideration-of-targets*.
18 See para.7 of the Memorandum: *http://www.legislation.gov.uk/uksi/2020/680/pdfs/uksiem_20200680_en.pdf*.
19 See *https://www.gov.uk/government/news/uk-announces-first-sanctions-under-new-global-human-rights-regime*.
20 Proceeds of Crime Act 2002 (POCA) s.362A(7).
21 POCA s.362I.
22 POCA s.362B.
23 POCA s.362A(1) and (2).
24 POCA s.362B(6)(c).
25 POCA s.362B(6)(b).
26 PEP refers to a person who is "or has been" entrusted with a public function by an international organisation or State, or who is a family member or close associate of such a person (POCA s.362B(7)). Guidance on who is a PEP is to be found in art.3(9) of the European Union's Fourth Anti-Money Laundering Directive, but the list is not exhaustive and it will be necessary to consider the nature of the person's power and influence.
27 "Serious crime" refers to offences set out in Sch.1 of the Serious Crime Act 2007 (including money laundering, tax evasion and bribery) (POCA s.362B(9)(a)).
28 "Connected" to a criminal suspect refers to a spouse, relative, relative of spouse and individuals acting together to exercise control of a company (Corporation Tax Act 2010 s.1122) (POCA s.362B(9)(b)).
29 The application can be made as one under s.362J of the POCA.
30 POCA s.362A(3).
31 POCA s.362G.
32 POCA s.362G.
33 POCA s.362F.
34 POCA s.362E(1).
35 POCA s.362C(1) and (2).
36 POCA s.362G(3) and (4).
37 POCA s.326G(5).
38 POCA s.362F(1).
39 Policing and Crime Act 2017 s.146 (1).
40 Policing and Crime Act 2017 s.146 (3).

41 However, separate transactions can also be assessed together. See para.12 of the Penalty Report at: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_*data/*file/876971/200331_-_SCB_Penalty_Report.pdf.*

42 See the OFSI guidance here: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708990/Monetary_Penalties_Guidance_web.pdf.*

43 See *https://www.gov.uk/government/collections/enforcement-of-financial-sanctions.*

44 Pursuant to the Policing and Crime Act 2017 s.147(3).

45 See the Penalty Report at para.18: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.*

46 See the Penalty Report at para.19: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.*

47 See OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, at *http://www.oecd.org/corruption/oecdantibriberyconvention.htm.* The OECD Convention has been signed by 44 countries, and it repeatedly references and discusses due diligence. The UN Convention Against Corruption, which has 140 signatories and 187 parties, similarly references the criticality of measures to prevent corruption. United Nations Convention Against Corruption, at *https://www.unodc.org/unodc/en/corruption/tools_and_publications/UN-convention-against-corruption.html.*

48 See, e.g., Order, In the Matter of Quad/Graphics, Inc., Admin. Proc. File No. 3-19531 (Sept. 26, 2019), at *https://www.sec.gov/litigation/admin/2019/34-87128.pdf*; Order, In the Matter of Walmart, Inc., Admin. Proc. File No.3-19207 (June 20, 2019), available at *https://www.sec.gov/litigation/admin/2019/34-86159.pdf*; Complaint, SEC v Teva Pharmaceuticals Ltd, No.1:16-cv-25298 (S.D. Fla. 22 December 2016); Plea Agreement, United States v Walmart, Inc. (June 20, 2019); In re: Bio-Rad Labs., Inc., Admin. Proc. File No.3-16231 (3 November 2014); States v Kozeny, 667 F.3d 122, 127–133 (2d Cir. 2011).

49 TRACE International, 2019 Global Enforcement Report, at 6, avaiable at *http://3afvm642sqoq9muh73hsqhtz-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/TRACE-Global-Enforcement-Report-2019.pdf*.

50 See, e.g., *Metal-Tech Ltd v Republic of Uzbekistan*, ICSID Case No.ARB/10/3) (2013); Lucinda Low and Jonathan Drimmer, "We'll Take That Mine: The Corruption Defense by Governments in International Arbitrations", 60 RMMLF-Inst. 20 (2018).

51 See, e.g., Peter Koven, "Former Centerra CEO 'Shocked" by lack of Canadian Action after Controversial Arrest in Bulgaria," Financial Post, 18 August 2015.

52 See, e.g., BlackRock, Business Conduct and Ethics, at *https://www.blackrock.com/corporate/responsibility/ethics-and-integrity* ("we conduct appropriate due diligence on our business partners according to the risks they present, including corruption risk").

53 See Canada's Enhanced Corporate Social Responsibility Strategy to Strengthen Canada's Extractive Sector Abroad, at *https://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/other-autre/csr-strat-rse.aspx?lang=eng*.

54 See, e.g., OECD Due Diligence Guidance for Responsible Business Conduct (2018), at *http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf.*

55 See, e.g., Brecken Branstrator, Gemfields Agrees to Pay $7.6M to Settle Mozambique Lawsuit, National Jeweler (30 January 2019), at *https://www.nationaljeweler.com/diamonds-gems/social-issues/7387-gemfields-agrees-to-pay-7-6m-to-settle-mozambique-lawsuit*; "BAT faces landmark legal case over Malawi families' poverty wages," The Guardian (31 October 2019), at *https://www.theguardian.com/global-development/2019/oct/31/bat-faces-landmark-legal-case-over-malawi-families-poverty-wages*; *Choc v Hudbay Minerals Inc.*, 2013 ONSC 1414 (22 July 2013).

56 See Human Rights and Environmental Disputes in International Arbitration, Kluwer Arbitration Blog (24 July 2018), *http://arbitrationblog.kluwerarbitration.com/2018/07/24/human-rights-and-environmental-disputes-in-international-arbitration.*

57 See FIN-2014-A008 (11 September 2014).

58 See FATF, Financial Flows from Human Trafficking (2018), at *http://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf.*

59 See Michael Janda and Peter Ryan, "Westpac faces fines over 'serious and systemic' anti-money laundering breaches, AUSTRAC says", ABC News, 19 November 2019, at *https://www.abc.net.au/news/2019-11-20/westpac-to-face-fines-anti-money-laundering-terrorism-breaches/11720474.*

60 See Equator Principles (July 2020), at *https://equator-principles.com/wp-content/uploads/2020/01/The-Equator-Principles-July-2020.pdf.*
61 See Peter J. Meyer, Congressional Research Service Report, U.S. Strategy for Engagement in Central America: Policy Issues for Congress (12 November 2019) at 1, 14.
62 See Canada's Enhanced Corporate Social Responsibility Strategy to Strengthen Canada's Extractive Sector Abroad, at *https://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/other-autre/csr-strat-rse.aspx?lang=eng.*
63 See UK Government Modern Slavery Statement, 26 March 2020, at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875800/UK_Government_Modern_Slavery_Statement.pdf.*
64 See *https://www.homeaffairs.gov.au/criminal-justice/Pages/modern-slavery.aspx.*
65 See, e.g., "BP Issues Detention Orders against Companies Suspected of Using Forced Labor", 1 October 2019, at *https://www.cbp.gov/newsroom/national-media-release/cbp-issues-detention-orders-against-companies-suspected-using-forced.*
66 See Rachel Davis & Daniel Franks, Costs of Company-Community Conflict in the Extractive Sector (2014), at 19, at *https://www.csrm.uq.edu.au/media/docs/603/Costs_of_Conflict_Davis-Franks.pdf.*
67 See Introductory Remarks by Commissioner Phil Hogan at OECD Global Forum on Responsible Business Conduct (19 May 2020), at *https://ec.europa.eu/commission/commissioners/2019-2024/hogan/announcements/introductory-remarks-commissioner-phil-hogan-oecd-global-forum-responsible-business-conduct_en.*
68 See, e.g., IHRB, Top 10 Business and Human Rights Issues, *https://www.ihrb.org/library/top-10/top-ten-issues-in-2020.*
69 For instance, France's Duty of Vigilance Law. Adopted in 2017 applies to large multinational companies—specifically: (a) those headquartered in France that employ at least 5,000 employees in France, or at least 10,000 employees worldwide (including through direct and indirect subsidiaries); or (b) foreign companies headquartered outside France, with French subsidiaries that employ at least 5,000 employees in France. Companies subject to the law must establish mechanisms to prevent human rights violations and environmental impacts throughout their chain of production, including those of their subsidiaries and companies under their control. These mechanisms must be reported each year as part of a "vigilance plan". See Loi no. 2017-399 du 27 Mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (27 March 2017).
70 See List of large businesses, associations & investors with public statements & endorsements in support of human rights due diligence regulation, *https://www.business-humanrights.org/en/list-of-large-businesses-associations-investors-with-public-statements-endorsements-in-support-of-human-rights-due-diligence-regulation.*
71 See Study on Due Diligence Requirements through the Supply Chain (25 February 2020), at *https://data.europa.eu/doi/doi:10.2838/39830.*
72 See Introductory Remarks by Commissioner Phil Hogan at OECD Global Forum on Responsible Business Conduct (May 19, 2020), at *https://ec.europa.eu/commission/commissioners/2019-2024/hogan/announcements/introductory-remarks-commissioner-phil-hogan-oecd-global-forum-responsible-business-conduct_en.*

Issue 179

Market Abuse Update

Authors: **Karen Anderson and Chris Ninan, Herbert Smith Freehills LLP**

Coverage

In the next issue of Compliance Officer Bulletin, the authors provide an overview of the Market Abuse Regulation and the latest updates on the FCA's interpretation of the regulation and Enforcement cases.

COMPLIANCE OFFICER BULLETIN

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

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

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

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

42672500