THE CITY LIBRARY

ISSUE 190 – October 2021

COMPLIANCE OFFICER BULLETIN

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

Philip Annett, Partner, London

Henry Garfield, Partner, London

Terence Gilroy, Partner, New York

Paul Glass, Partner, London

Amy J. Greer, Partner, New York

Jennifer L. Klass, Partner, New York

Mark Simpson, Partner, London

Charles Thomson, Partner, London

Kimberly Everitt, Knowledge Lawyer, London

Mark Banks, Senior Associate, London

Lereesa Easterbrook, Senior Associate, London

Mary Jordan, Senior Associate, London

Chris Whalley, Senior Associate, London

Sarah Williams, Senior Associate, London

Rosanne Hooper, Associate, London

Ben Thatcher, Associate, London

Lauren Chapple, Trainee, London

Samantha Lee, Trainee, London

Financial Crime Update

1. Reviewing the EU and UK AML regime proposals: What firms need to know

1.1 Introduction

As responses to the pandemic stabilise and the regulatory landscape begins to approach normality, regulators have indicated a shift in focus from crisis intervention to a more stable outlook on reforming regulatory frameworks.

On 20 July 2021, the European Commission presented a package of legislative proposals establishing a new framework for the EU's anti-money laundering and countering terrorism financing ("AML/ CTF") regime. The package will create an EU-wide AML supervisory authority, establish a new directly applicable single rulebook, and extend the scope and requirements of the regime including, significantly, to all cryptoasset service providers.

Shortly after, on 22 July 2021, HM Treasury ("HMT") issued both a call for evidence and consultation on the UK's AML framework. The consultative documents both look into different mechanisms which will enable firms to take a risk-based approach to their internal controls, instead of being restricted by the various requirements set out

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

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

in within the current UK regulatory framework. These proposals could implement wide-ranging changes to the UK's AML/CTF regime whilst maintaining international standards set by the FATF.

This section explores the proposals from the Commission and HMT in more detail, and also sets out considerations for UK firms.

1.2 The EU framework proposals

The legislative package, part of the Commission's AML/CTF Action Plan, follows a number of longstanding concerns about the existing EU AML/CTF regime. Ineffective and insufficient implementation of the existing regime across EU Member States has contributed to inconsistent enforcement of rule breaches. EU rules have been transposed and applied in a divergent manner across Member States, leading to significant variation in transparency, supervisory oversight and enforcement powers granted to Financial Intelligence Units ("FIUs"). The current regime is also inadequate at dealing with suspicious activities and transactions in cross-border circumstances. These concerns were echoed on 28 June 2021 by the European Court of Auditors, which highlighted weak enforcement of the existing rules, noting that EU bodies have limited tools to ensure the appropriate and consistent application of the AML/CTF regime and, further, there is generally poor coordination between Member States when taking enforcement action.

Further, the existing EU AML/CTF regime is not fully consistent with the latest international standards that have evolved since the last amendment to the framework, meaning that the current rules are also ineffective in dealing with new threats arising from innovation. This issue is particularly acute in relation to illicit cryptocurrency activity in the EU, in light of the October 2018 recommendations of the Financial Action Task Force ("FATF") relating to cryptoassets.

To address these concerns, the Commission has published the following package of legislative proposals:

- a proposal for a regulation establishing a new EU-wide AML/CTF authority;
- a proposal for a new regulation on directly applicable rules such as customer due diligence (also known as the new single rulebook);
- a proposal for a 6th AML Directive ("MLD6"), to replace MLD5 and MLD4; and
- a proposal for a revised Regulation 2015/847/EU on the transfer of funds (Wire Transfer Regulation or "WTR"), to make it possible to trace transfers of cryptoassets and limit large cash payments.

The package is designed to bring harmonisation throughout the EU in terms of how the rules are applied, interpreted and enforced. The proposals will:

- create a centralised EU AML/CTF authority;
- provide a new single rulebook for AML/CTF compliance; and
- expand the scope of the AML/CTF regime to apply fully to the cryptoassets sector.

1.2.1 New EU Anti-Money Laundering Authority

The new EU Anti-Money Laundering Authority ("AMLA") will serve as the EU's central authority for AML/CTF supervision, assuming responsibility for the European Banking Authority's current related competences. The AMLA will have certain direct and indirect supervision remits, and will facilitate cooperation among EU FIUs. To achieve its objectives, the AMLA will be tasked with a large number of responsibilities, including:

- directly supervising certain of the "riskiest" obliged entities, ensuring group-wide compliance with the requirements set out in the AML/CTF framework (including any other legally binding EU acts that impose AML/CTF-related obligations on financial institutions) through supervisory reviews and assessments. These obliged entities include high-risk cross-border credit and financial institutions with activity in a significant number of Member States, selected periodically, and, in exceptional cases, any entity whose material breaches of applicable requirements are not sufficiently or in a timely manner addressed by its national supervisor;
- carrying out periodic reviews of Member State financial supervisors, facilitating colleges and coordinating information exchange;
- coordinating peer reviews of non-financial supervisors, requesting non-financial supervisors to investigate possible breaches of requirements and to consider imposing sanctions or remedial actions, and carrying out periodic reviews;
- supporting and coordinating the work of FIUs and contributing to improved cooperation between FIUs, including joint analyses, specialised training, expert knowledge and threat assessments; and
- adopting and implementing regulatory technical standards, guidelines and recommendations, adopting binding decisions, administrative measures, and pecuniary sanctions towards directly supervised obliged entities, and issuing to Member State supervisory authorities requests to act and instructions relating to the exercise of their own supervisory powers.

1.2.2 The EU single rulebook

The single rulebook will act as a unified AML/CTF framework that includes directly applicable rules on the AML/CTF requirements. To address concerns about divergent Member State transposition of current obligations set out in the existing AML directives, the Commission's proposal for a single rulebook is set out in a regulation, providing detailed requirements that will directly apply in Member States to obliged entities. The single rulebook will be supported by a number of regulatory technical standards to be prepared by the AMLA.

In addition to those who are already obliged entities under the present regime, the single rulebook will expand the list of obliged entities to include:

- all types and categories of cryptoasset service provider. The definitions of cryptoasset and cryptoasset service provider are aligned to those set out in the proposed Regulation on Markets in Cryptoassets;
- crowdfunding service providers that are not within the scope of the Crowdfunding Regulation ((EU) 2020/1503);
- mortgage credit intermediaries and consumer credit providers that are not financial institutions; and
- operators of investor residence schemes (those working on behalf of third-country nationals to obtain a residence permit to live in an EU country).

The new rulebook will also make substantial changes to existing requirements, including:

- clarification of requirements relating to internal policies, controls and procedures, including group obligations and requirements that apply to parent entities which are not themselves obliged entities;

- granular requirements in respect of customer due diligence obligations and identity verification, including the use of electronic identification (intended to align with the Commission's Digital Finance Strategy and proposed framework for a European Digital Identity);
- a more granular and proportionate approach to the identification of high-risk jurisdictions: "black list" jurisdictions (in principle, those third countries "subject to a call for action" by the FATF) will be subject to all enhanced due diligence measures and to additional country-specific countermeasures, while "grey list" jurisdictions (in principle, those third countries "subject to increased monitoring" by the FATF) will be subject to country-specific enhanced due diligence measures;
- additional requirements relating to Politically Exposed Persons ("PEPs");
- clarification of beneficial ownership requirements and new requirements relating to nominees and foreign entities;
- guidance on the identification and reporting of suspicious transactions, including a harmonised template, and guidance on the red flags that should raise suspicion;
- requirements for the processing of certain categories of personal data, including a five-year period for data retention; and
- an EU-wide limit of €10,000 on large cash payments.

Further significant changes to the current AML/CTF regime are set out in other proposals within the Commission's package. The Commission's proposed MLD6 provides for the interconnection of existing Member State bank account registers through a single access point, to be developed and operated by the Commission. Proposed amendments to the WTR will expand scope of the FATF's recommendation 16—the "travel rule"—to cryptoassets, requiring cryptoasset service providers to obtain, hold and share required and accurate information on cryptoasset transfers users and make that information available on request to appropriate authorities.

The AMLA will have the power to impose administrative pecuniary sanctions and periodic penalty payments. Decisions on sanctions and penalties will be appealable to the Court of Justice of the European Union, which may annul, reduce or increase the fine or periodic penalty payment imposed.

1.2.3 Next steps

The AMLA is expected to be established in 2023 and operational by 2024, with the activity of direct supervision to commence at the beginning of 2026. Direct supervision will start once the single rulebook applies in Member States. The rulebook, including technical standards, is expected to be in place and apply by the end of 2025.

Firms may wish to review their AML risk assessment policies and procedures with a view to the new framework; firms can consult Annexes I, II ,and III of the single rulebook proposal to review the Commission's proposed non-exhaustive list of risk variables and factors evidencing potentially lower or higher risk.

More broadly, it will be critical for firms to understand how direct supervision by the AMLA will work in practice, both in terms of entities falling within scope and the role that Member State supervisors will play in AML supervision and enforcement. Directly supervised entities will be those operating cross-border in multiple Member States with a "high inherent risk profile", to be determined by methodology based on the risk factor categories related to customer, products, services, transactions, delivery channels and geographical areas. This methodology will be set out in regulatory technical standards developed by the AMLA by 1 January 2025. The Commission also proposes that supervision of entities directly supervised by AMLA will be undertaken by joint supervisory teams led by the AMLA and including staff of Member State supervisory authorities; however, while it is clear that the Commission intends for the AMLA to take the role of primary AML supervisor for directly supervised entities, the boundaries of any dual regulation or enforcement regime remain unclear at this stage. Firms should keep a watching brief on these issues as they develop further.

1.3 Considerations for UK firms, including HM Treasury's consultations

UK firms with EU parent undertakings should expect to comply the proposed single rulebook's expanded group-wide requirements. While UK firms without an EU nexus will not be caught by the direct application of the proposals, a similar review of the AML/CTF framework is underway in the UK, and though the final structure of the UK's framework may not match the EU's proposals, alignment with FATF standards (a stated aim of the UK's review) will naturally converge the two regimes to an extent. On 22 July 2021, HMT published two consultative documents on the UK's AML framework:

- a call for evidence on the review of the UK's AML/CTF regulatory and supervisory regime; and
- a consultation on amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLRs").

1.3.1 Call for Evidence: Review of the UK's AML/CTF regulatory and supervisory regime

The call for evidence supports the review which will aim to assess the UK's AML/CTF regulatory (the MLRs and Office for Professional Body Anti-Money Laundering Supervision ("OPBAS") Regulations) and supervisory regimes. The call for evidence looks at three themes:

- a systemic review of the overall effectiveness of the regimes and their extent (i.e. the sectors in scope as relevant entities);
- a regulatory review of whether key elements of the current regulations are operating as intended; and
- a supervisory review of the structure of the supervisory regime, including the work of OPBAS to improve effectiveness and consistency of supervision.

This review is part of HMT's legal requirements: the MLRs require HMT to publish a report no later than 26 June 2022 reviewing the regulatory provision set out in the MLRs and OPBAS Regulations, which must set out the objectives intended to be achieved, assess the extent to which the objectives are achieved, assess whether the objectives remain appropriate, and assess the extent to which they could be achieved in another way which involves less onerous regulatory provision.

HMT is also undertaking this review in the context of UK regulation post-Brexit, stating that it intends to maintain efforts to uphold FATF international standards, in particular the application of a risk-based approach to applying the AML/CTF regulatory framework, but aims to improve the effectiveness of the UK system, in line with FATF's own rebalancing towards measuring effectiveness rather than technical compliance. This rebalancing of effective outcomes versus technical compliance is a theme embedded throughout all of HMT's post-Brexit regulatory reviews.

1.3.1.2 Systemic review

HMT proposes breaking the systemic review into three key areas to form a judgment on how well the current UK regulatory regime effectively prevents money laundering and terrorist financing; considering the effectiveness of the system, the extent of its application and the evidence of enforcement action being taken.

The review aims to bottom out a common critique of the MLRs: that they drive the regulated sector to spend too much time and money on mandatory requirements rather than focusing on activities which more meaningfully and effectively contribute to removing bad actors and preventing illicit transactions. Among the topics of discussion on the review scope, the FCA is calling for input on the scope of regime (discussed further below), enforcement powers and the role of further guidance. From an enforcement perspective, the call for evidence asks stakeholders to consider whether the relatively low number of prosecutions under the MLRs may represent an enforcement failing; an area that has also been an FCA focus.

1.3.1.1 Regulatory review

As part of the regulatory review, HMT intends to look at the effectiveness of particular elements of the MLRs and their application in the AML/CTF regime.

In particular, the review looks at the risk-based approach—asking whether the risk-based approach and the supervisory expectations in this regard are well understood. HMT recognises that whilst the risk-based approach allows flexibility, there are barriers which may need to be addressed—e.g. lack of understanding or concerns about compliance leading to overly restrictive approaches. The FCA has, on multiple occasions, recognised that firms struggle to act within the boundaries of the current regime and therefore has encouraged the risk-based approach (see, for example, the FCA's expectations on how firms should apply their financial crime systems and controls during the pandemic, and its supervisory approach to cryptoasset businesses under the MLRs).

HMT also touches on new technologies and how these interact with existing regulations. Stakeholders are asked to provide input on whether the MLRs prevent the adoption of useful new technologies (such as digital identities) and whether there are further steps needed to increase adoption of technologies that mitigate financial crime risk.

Finally, the call for evidence looks at the gatekeeping function of supervisors under the MLRs and the different tests they have developed to review, assess and approve new entrants. HMT has identified that different tests and standards are applied and asks stakeholders to consider whether existing tests cumulatively act as an effective gatekeeping system, and whether a more harmonised or detailed system is required. HMT specifically calls out the detailed requirements set out by the FCA for new cryptoasset businesses, which have acted as a quasi-authorisation process, requiring firms to provide significant levels of information to the FCA before obtaining supervisory approval.

1.3.1.2 Supervisory review

Finally, HMT considers the overall effectiveness surrounding the structure of the supervisory regime (found to be moderately effective by FATF), including both statutory and professional body supervisors, the strengths and weaknesses of the regime, particularly any supervisory gaps which result from the structure, and possible options for reform, for example consolidation of the supervisory bodies or the creation of a single body with oversight of the whole regime.

1.3.2 Consultation: Amendments to the MLRs

In its consultation on the MLRs, HMT proposes to amend the MLRs to make some time-sensitive updates, which are required to ensure that the UK continues to meet international standards set by the FATF, whilst also clarifying how the AML regime operates. These updates include:

- changes in scope to reflect latest risk assessments, in particular to exempt particular payment service providers which may present a low risk of money laundering;
- clarificatory changes to strengthen supervision by allowing AML/CTF supervisors to have a right of access to view the content of a suspicious activity report ("SAR"), and to align the definition of credit and financial institutions with existing financial services legislation;
- expanded requirements to strengthen the regime, including among other changes expansion to proliferation financing;
- improving the effectiveness of the intelligence and information sharing gateway, and giving further supervisory powers to the FCA; and
- implementing the travel rule for cryptoasset transfers.

Some of the more significant changes are considered below.

1.3.2.1 Changes in scope to reflect latest risk assessments

The consultation seeks views on specific amendments to the scope of the regulated sector to exempt particular payment service providers which may present low risk of money laundering and terrorist financing. The potential activities for exclusion are account information service providers ("AISPs"), bill payment service providers ("BPSPs"), and telecom, digital, and IT payment service providers ("TDITPSPs"). Payment initiation service providers ("PISPs") have been suggested for exclusion from the regulated sector, but this consultation also seeks views on the potential risks presented by PISPs.

The proposed change in scope is focused on reducing cost and burden for both firms and supervisors in sectors where there is a low risk of money laundering and terrorist financing based on the UK risk assessment.

1.3.2.2 Strengthening supervision and information sharing & gathering

HMT has asked for views on the merits of amending the MLRs to explicitly allow for AML/CTF supervisors to have a right of access to view the content of a SAR submitted by their supervised population(s) on request. The government is also seeking views on the potential impacts and concerns that this requirement may pose to affected firms and individuals.

The consultation also seeks feedback on whether the activities that make a person a credit and financial institution as per reg.10 of the MLRs should be amended to align with the Financial Services and Markets Act 2000 ("FSMA") and defined terms under the Regulated Activities Order. HMT is considering whether an amendment to the wording of the MLRs could provide clarity for relevant persons who already fall under FSMA. The government is also seeking views on which activities do not currently have clarity on whether they fall in scope of the MLRs, to ensure this can be addressed.

Further, the consultation asks for feedback on amendments to the MLRs to improve the effectiveness of the intelligence and information sharing gateway, particularly on whether it would be beneficial for existing gateways under the MLRs be expanded to allow for reciprocal protected sharing from relevant authorities (including law enforcement) to supervisors.

1.3.2.3 Transfers of cryptoassets

Finally, as with the European Commission, HMT considers that the time is now right to begin planning for the implementation of the FATF travel rule for cryptoasset transfers, i.e. the extension of the requirement to provide originator and beneficiary information to transfers of cryptoassets. The government's approach to implementation is guided by the principle that the application of FATF recommendation 16 should be consistent across the financial services industry, regardless of the technology being used to facilitate transfers, unless there is a compelling reason to adopt a different approach. The requirements will apply to cryptoasset exchange providers and custodian wallet providers which are carrying on business in the UK.

HMT proposes to implement these requirements through amendments to the MLRs, rather than separate legislation as is the case for bank transfers, which has the benefit of consolidating AML legislation for the cryptoasset sector in one place. The consultation acknowledges that the process of integrating the travel rule requirements may take time and that a proportionate response is required and grace period for implementation has been proposed, with stakeholders asked to comment on length of any grace period granted. In the same vein of proportionality, the consultation also proposes to set a de minimis threshold of £1,000, below which more limited information will be required. This will be a fiat amount so firms will need to take a reasonable and justifiable approach to calculating the value of the transfer.

Extension of the travel rule is driven by international standards but ties in with the current UK focus on cryptoassets in both the financial crime and regulatory sector. As mentioned, the UK has taken a rigorous approach to cryptoasset firms seeking registration for AML purposes, which has led to long delays in FCA processing of applications and the high-profile rejection of Binance Markets Ltd's application.

1.3.3 Next steps

Responses to the call for evidence and consultation are due by 14 October 2021. HM Treasury proposes that firms will be allowed a grace period after the amendments to the MLRs are made, to allow the integration of compliance solutions.

It is clear that business-as-usual AML and CTF measures are once again in focus in the UK, with proposed changes looking to taking advantage of the post-Brexit position and improve the effectiveness of the UK regime in line with international standards. Whilst changes in the area of cryptoassets will increase obligations on firms, the proposals are more generally aimed at reducing the burden of regulation in low-risk sectors, focusing efforts on meaningful activities and improving supervision, all with the aim of ensuring the UK's AML/CTF regime remains strong and deterrent, aligned with international standards, and proportionate to the needs of the market.

2. Emerging themes in the DPA landscape

2.1 Introduction

The guidance on Deferred Prosecution Agreements ("DPAs") published by the Serious Fraud Office ("SFO"), and recent DPAs entered into with the SFO, provide a pathway for companies to follow should they identify criminal conduct in their company which could cause the company itself to be held criminally liable. The SFO has been actively using DPAs to hold companies accountable for their actions since their introduction on 24 February 2014. This section will consider the DPA landscape by examining the SFO's guidance and looking at some themes we have identified from the recent DPAs entered into with the SFO.

The SFO continues to take the lead on investigating and prosecuting serious and complex financial crime cases including bribery, corruption and fraud. In recent years there has been a steady increase in the number of DPAs entered into by the SFO and companies under investigation for criminal offences. In light of such an increase, the SFO published guidance on DPAs on 23 October 2020, adding to its publicly available Operational Handbook. The guidance should be read alongside the DPA Code of Practice which was published when the DPA regime was introduced in 2014. This section will look at the approach adopted by the SFO and analyse what companies should expect when faced with a criminal investigation. We will consider the guidance itself and some recent examples of DPAs entered into with the SFO.

2.2 What is a DPA and what is the SFO's approach to DPAs?

A DPA is an agreement entered into between the SFO and a company where corporate criminal liability under the "directing mind" principle (by imputing guilt[1] through dishonest acts and intentions of representatives) has been established. A DPA, which must be approved by the courts, suspends a prosecution for a defined period of time and imposes conditions on legal entities requiring them to rectify criminal activities and misconduct. The SFO views DPAs as a "valuable tool in the fight against serious fraud, bribery and corruption, capable of not only punishing corporates for criminality but also making sure the company rehabilitates and becomes a better corporate citizen. This helps [the SFO] foster a business environment where everyone plays by the rules".[2] The SFO, with its continued focus on corporate entities, has entered into 12 DPAs since 2014 at an increasing frequency, demonstrating its desire to hold companies accountable by using the threat of prosecution to reach a negotiated settlement.

2.3 SFO DPA guidance

The guidance on DPAs sets out how the SFO intends to continue using DPAs proactively to combat financial crime. The guidance does not introduce any novel concepts but rather focuses on the SFO's continued approach, setting the tone and expectations that companies ought to consider before entering into DPA discussions with the SFO and during the negotiations.

Interestingly, the guidance was originally an internal document, but was subsequently published as a sign of the SFO's transparent approach, continuing its efforts to encourage companies to cooperate when potential criminal conduct is identified. The guidance covers the following:

- the SFO's negotiation process;
- parallel investigations;
- the invitation to enter into a DPA;
- the terms of negotiations;
- DPA disclosure;
- DPA terms;
- financial penalties; and
- statements of facts and agreement.

We will examine a few key areas of the guidance and consider what factors companies should have in mind when engaging with the SFO.

2.3.1 Tests: Evidential and Public Interest

The SFO must apply two tests when entering into a DPA, the evidential test and the public interest test. The evidential test lies at the heart of the DPA process and requires "sufficient evidence to provide a realistic prospect of conviction",[3] or if the realistic prospect is not met yet, there needs to be "at least a reasonable suspicion based upon some admissible evidence that the Company has committed an offence … and reasonable grounds for believing that a continued investigation would provide further admissible evidence within a reasonable time".[4] The public interest test means that the SFO must perform a balancing act and must be satisfied that it would be in the public interest to enter into a DPA, weighing up the advantages and disadvantages of a DPA against those of a prosecution. Some examples of public interest factors include the historical conduct of the company, established company practices, the time period over which an offence was committed, how a company conducts itself when self-reporting, and any impact the decision will have on the general public. Importantly, while DPAs must be approved by the Crown Court, the Court's role in examining the evidential basis of the offence is limited. As a Edis LJ made clear in the recent DPA involving Amec Foster Wheeler Energy Ltd:

> "In a DPA application, the court is concerned with two areas of factual material: that concerning the commission of the offences; and that concerning the situation and conduct of the suspect after the offences were committed, during the investigation and its current situation. In neither area can the court make any findings of fact. It is dependent on the information with which it is supplied, and relies on the prosecutor to make enquiries and to satisfy itself that the court is being asked to proceed on an accurate statement of the relevant facts."[5]

A company should therefore be satisfied that the SFO has sufficient evidence that a criminal offence has been committed before entering into detailed DPA discussions.

2.3.2 Cooperation and negotiation

Cooperation, according to the SFO's guidance, is "providing assistance to the SFO that goes above and beyond what the law requires".[6] The guidance explains how companies ought to self-report at a reasonable time and commence a conversation with the SFO if there is knowledge or suspicion of misconduct. A non-exhaustive list of examples of cooperation includes: "… reporting within a reasonable time of wrongdoing coming to light; taking remedial actions; preserving evidence and providing it promptly; identifying witnesses and providing their accounts; providing an internal investigation report; and waiving privilege …" (although this cannot be compelled; see below).[7]

In respect of complicated corporate structures, the guidance acknowledges that a parent company may not always have complete oversight of a subsidiary. This is reflected in the guidance by the fact that if a parent company becomes aware of criminal activity in a subsidiary, reaches out to the SFO and chooses to cooperate, the SFO can "address the letter of invitation to the parent even if it is anticipated that the terms of any DPA would be limited to the subsidiaries".[8] This demonstrates how the SFO is willing to work with companies who are prepared to self-report misconduct and rectify it, even if the misconduct is not immediately visible to the "directing mind" of the parent company.

With regard to cooperation, the issue of legal privilege in the negotiations remains a hot topic. Where a claim for legal privilege over documentation can be properly established, waiving privilege is not considered a mandatory requirement of cooperation, so a company can choose not to waive privilege when providing material to the SFO. This is covered in the guidance where it explains that a company cannot be penalised for refusing to provide privileged material.[9] Refusing to waive privilege therefore cannot be viewed negatively during negotiations but in order to maintain privilege, a company must ensure that: (i) the privilege is properly established; and (ii) certification by independent counsel is provided for the privileged documents.

2.3.3 Self-reporting: What is a reasonable time to report?

The SFO does not provide a definition for "reasonable" in relation to self-reporting, despite frequently using the term to explain timeframes when companies ought to self-report. When companies are considering self-reporting this ambiguity in the guidance is unhelpful where companies need to balance the real risk of not self-reporting early enough, with the potential to create a major problem out of a small issue by alerting the SFO too early before conducting any internal investigations. The section on self-reporting in the guidance says: "voluntary self-reporting suspected wrongdoing [should occur] within a reasonable time of those suspicions coming to light."[10] In practice this means that the self-reporting should occur before the SFO discovers evidence of wrongdoing through detailed investigations and the information should be provided voluntarily, "... without the threat of imminent disclosure by third a party ...".[11] The SFO anticipates that companies will conduct a certain degree of internal investigation before deciding to self-report, so a reasonably confined internal investigation will be viewed positively in any future discussions. Moreover, conducting an internal investigation is one way that a company can demonstrate early cooperation with the SFO by providing a report following an internal investigation including source documents. This report can also form the basis of the terms of a DPA.

2.3.4 Breach of a DPA

Once a DPA is in place, the SFO expects a company to maintain its good behaviour and to work to eliminate all misconduct. The guidance examines a company's failure to comply with a DPA, delving into what actions the SFO can take against an offending company. Whilst there have not yet been any breaches of any of the DPAs, the guidance makes it clear that the SFO will not hesitate to approach the courts to vary DPAs or to invite the court to consider alternative disposals. This section of the guidance is clearly designed to act as a deterrent, by outlining the consequences of a breach, including the option of applying to the court to lift the suspension of the indictment and to reconsider criminal proceedings.

2.4 Recent DPAs: What can we learn?

Under Lisa Osofsky's stewardship, the SFO has significantly increased its use of DPAs to combat financial crime with no signs of slowing down. Eight DPAs have been entered into in the last three years, in contrast to four DPAs in the three years prior to Ms Osofsky's appointment. Since the publication of the guidance, two DPAs have been entered into with Airline Services and Amec Foster Wheeler Energy Ltd with two DPAs announced in late July 2021. We will examine the DPAs involving Airbus, Airline Services Ltd and Amec Foster Wheeler Energy Ltd to further understand what the SFO seeks from a company when entering into negotiations.

2.4.1 Airbus DPA

The Airbus DPA was the first DPA of 2020 and remains the most significant as it captures the key points on what companies need to consider when deciding whether to negotiate with the SFO. The Airbus DPA attracted a total penalty of €3.6 billion for bribery and corruption in relation to investigations by three different prosecuting authorities (the SFO, the French Parquet National Financier ("PNF") and the US Department of Justice ("DOJ")).

The Airbus DPA requires Airbus to, inter alia: (i) fully and honestly cooperate with all authorities involved in the investigation; (ii) retain all materials for the term of the DPA (these included materials related to internal investigation and materials collected by the authorities); (iii) aid the authorities' requests for interviews and disclosure of documents that were not protected by any type of legal privilege; and (iv) immediately report any evidence of criminal activity.

Some of the actions which Airbus independently undertook to successfully conclude the DPA included:

- improving its compliance teams and replacing senior management at the executive committee level;
- introducing an independent sub-committee of the board overseeing ethics and compliance of the Airbus group;
- bringing in a new Chief Compliance Officer and General Counsel;
- revising its Code of Conduct and implementing training across the Airbus group;
- standardising good practice within the Airbus group across all jurisdictions in which Airbus operates;
- using external compliance experts that only answer to the executive committee; and
- creating an environment that focuses on stronger credit and contractual governance.

Airbus' voluntary undertakings resulted in a change in its culture and practice and were interpreted by the SFO as clear evidence of cooperation.

2.4.2 Airline Services Ltd

The Airline Services Ltd DPA was approved in October 2020 with a 50% discount on the penalty because Airline Services Ltd had cooperated with the SFO since its initial self-report. One of the most notable decisions taken by Airline Services Ltd's board was to keep the dormant, non-trading company as a shell company so that they could comply with the DPA obligations. Cooperation with the SFO was clear, with the company facilitating interviews and providing materials to the SFO and identifying deficiencies in its compliance programme.

2.4.3 Amec Foster Wheeler Ltd

The Amec Foster Wheeler Ltd DPA in July 2021 resulted in a heavier financial penalty due to the gravity of the offences committed by former employees and the decision taken back in 2007 by its board to not self-report. Despite these factors, a DPA was approved on the basis of positive steps taken by the parent company, John Wood Group Plc, after they acquired Amec Foster Wheeler Ltd and during its engagement with the SFO. This DPA demonstrates consistency with the new guidance where a parent company will have the opportunity to work with the SFO if it is prepared to take responsibility for and rectify conduct by a company within the corporate structure.

These three DPAs clearly demonstrate that cooperation and good behaviour can fundamentally impact the terms of a DPA. Companies that have uncovered criminal conduct and are considering approaching the SFO should consider both the guidance and the key documents from the historic DPAs before they do so.

2.5 Predictions for the future: Potential expansion of corporate criminal liability

Despite the SFO's successes in securing a number of DPAs, they have expressed a desire to widen their powers through the introduction of further "failure to prevent" offences (similar to the UK Bribery Act s.7 offence of "failure to prevent bribery") in respect of other economic crimes. The Law Commission recently consulted on possible options for reforming[12] the law on corporate criminal liability with one option being an expansion of the "failure to prevent" regime to include, for example, offences of failure to prevent money laundering and failure to prevent fraud. Other options under consideration include adopting a civil-based administrative penalty approach or adopting the US vicarious liability model were companies can be held criminally liable for offences committed by an employee. The outcome of the consultation will be published later in the year and should any legislative reform be proposed, we would not expect anything on the statute book for some time.

2.5.1 Concerns over the DPA regime

In its discussion paper, the Law Commission identifies four concerns relating to the accountability and reliability of DPAs[13] as they anticipate that if any reforms on corporate criminal liability are forthcoming, there will be a considerable increase in the number of DPAs. In particular, concern is raised as to the fairness of the DPA regime and "whether the potential commercial and reputational consequences of a criminal conviction were such that corporations were too strongly incentivised to enter into DPAs, or to undertake to meet the financial commitments of DPAs entered into by a subsidiary, despite having a potentially meritorious defence".[14] This goes to the point made above, that companies must be satisfied that there is sufficient evidence of criminal wrongdoing before entering into DPA discussions.

3. Developments on the Cum-Ex dividend scandal

3.1 Background

Cum-Ex trading (also known as dividend arbitrage) is a practice that involves complex trading prior to dividend payments enabling multiple parties to claim refunds for withholding tax that has only been paid once. In essence, shares are sold or swapped (often temporarily) prior to a dividend payment in order to produce two tax refunds on one set of shares. It is estimated that between 2002 and 2012 European tax authorities were deprived of approximately €55 billion through Cum-Ex trades. The countries most affected by the Cum-Ex scandal are Germany, Denmark, Italy, and France. A number of European tax authorities, most notably Germany and Denmark, are pursuing investigations and charges against firms and professionals who participated in the schemes.

Although the tax loophole did not exist in the UK, many of the individuals involved in the scheme were UK nationals and much of the trading is likely to have taken place in the City of London. This has resulted in the Danish authorities choosing to bring their claims in the UK and the Financial Conduct Authority ("FCA") taking its own regulatory action.

3.2 Developments in the English Courts

SKAT, the Kingdom of Denmark's tax revenue agency, contends that Sanjay Shah, founder of Solo Capital Partners LLP ("Solo Capital"), is the "mastermind" of the Cum-Ex dividend scandal. As a result, he is at the centre of the litigation that SKAT has brought in the English High Court (*Skatteforvaltningen (the Danish Customs and Tax Administration) v Solo Capital Partners LLP (in special administration)* [2021] EWHC 974 (Comm)).

SKAT brought 5 civil claims against around 114 individual and corporate defendants in a complex set of proceedings in the UK High Court that was anticipated to be one of the lengthiest trials of recent years. SKAT had claimed damages equivalent to £1.5 billion alleging that the defendants, Solo Capital and a number of others, operated a fraudulent scheme between 2012 and 2015 that resulted in SKAT issuing billions of pounds worth of wrongful tax rebates.

However, on 27 April 2021, the Commercial Court dismissed the SKAT's claim against Solo Capital. Mr Justice Andrew Baker dismissed the claim on the grounds that the claim for the repayment of the withholding tax contravened "Dicey Rule 3", also known as the "Revenue Rule", which stipulates that English courts cannot enforce a revenue law of another jurisdiction. The Danish authorities contended that their claim was civil in nature and intended to recover the proceeds of fraud, but Mr Justice Baker found that the claims were an indirect enforcement of a sovereign right and thereby forbidden under the "Revenue Rule". Put simply, the Danish tax authority cannot use the English courts as a mechanism to enforce its own tax laws.

SKAT has been granted limited permission to appeal on its jurisdictional arguments in which it contends that the prohibition under the "Revenue Rule" should be set aside so as not to "derogate from and impair the effectiveness of the Brussels-Lugano regime". They argued that the regime provides for the mutual recognition and enforcement of civil and commercial judgments and therefore if the claims are considered civil or commercial matters, then the prohibition under the "Revenue Rule" should be set aside. Mr Justice Andrew Baker rejected this argument at first instance; although he agreed that the claims were civil or commercial in nature, he held that the "Revenue Rule" was an "overriding rule of English law" and is not disapplied by the Brussels–Lugano regime.

It will be interesting to see how SKAT's appeal progresses, but the High Court decision may serve, at least temporarily, as a roadblock to the UK enforcement efforts of EU tax authorities in the wake of the Cum-Ex scandal.

3.3 FCA enforcement action

On 24 February 2021, the FCA was ordered to halt its investigation into a trader involved in the European Cum-Ex dividend scandal pending the outcome of the SKAT's litigation in the High Court (as discussed above). However, following the dismissal of the SKAT's claim the FCA has been able to proceed with its enforcement action.

Accordingly, in May 2021 the FCA issued its first penalty in relation to the Cum-Ex trading scandal to Sapien Capital Ltd ("Sapien"), a corporate finance advisory and brokerage firm. The fine of £178,000 (reduced from £236,740) was imposed for failings that led to the risk of facilitating fraudulent trading and money laundering.

The FCA found Sapien to have failed in its duty to have in place adequate systems and controls to identify and mitigate the risk of being used to facilitate fraudulent trading and money laundering in relation to business introduced by the Solo Group. The FCA noted that the way these trades were conducted by the Solo Group and their clients, in combination with their scale and volume, were highly suggestive of sophisticated financial crime, and appear to have been undertaken to create an audit trail to support withholding tax reclaims in Denmark and Belgium. The FCA also stated that Sapien had failed to exercise due skill, care and diligence in applying anti-money laundering policies and procedures and in failing properly to assess, monitor and mitigate the risk of financial crime in relation to clients introduced by the Solo Group and the purported trading.

The FCA considered the breach particularly serious given what it saw as Sapien's disregard for blatant red flags and its willingness to cut corners both in relation to on-boarding due diligence and ongoing monitoring when those red flags arose from the trading activities of the Solo Group and their clients.

The FCA's approach is notable as it focuses on Sapien's failings in its risks and controls to prevent fraudulent trading and money laundering, rather than the trading itself, which perhaps suggests a reluctance to make a decision as to the legality of Cum-Ex trading. The FCA has therefore found a way to penalise those involved in Cum-Ex trading without having to address its legality or even prove that the trades occurred. This enforcement approach, coupled with the fact that the FCA's fine is the first Cum-Ex enforcement action taken by a regulator outside of a country where the tax rebates were wrongfully claimed, may well pave the way for other regulators to pursue similar actions.

An information request from earlier this year confirmed that there were 14 firms and 8 individuals subject to investigation by the FCA in relation to the Cum-Ex scandal. In its statement on 6 May 2021 the FCA confirmed that its investigation into the involvement of UK based brokers in Cum-Ex dividend arbitrage schemes is continuing. This is in line with the FCA's stated intention to being a more assertive regulator. FCA enforcement markedly declined during the past year, likely as a result of the pandemic, however, it is clear from the FCA's 2021/2022 Business Plan that the FCA intends to be a more proactive and assertive regulator and to test the limits of its powers.

In the wake of the High Court's dismissal of SKAT's claim, and while the appeal is pending, it is for now unclear when, and how, the FCA will proceed with its investigations and enforcement efforts in relation to Cum-Ex trading. But it will certainly be interesting to see whether the FCA continues with the approach to enforcement seen in the Sapien case, focussed on systems and controls failures and the exercise of due skill, care and diligence, or if it will start bringing criminal prosecutions for the Cum-Ex trading itself, in line with its assertiveness agenda.

3.4 Concluding remarks

It is likely that the wave of enforcement in relation to the Cum-Ex dividend scandal will continue both in the UK and across Europe. German authorities, who have concluded that Cum-Ex trading likely constitutes tax evasion, are said to be investigating around 1,000 suspects, with the first German banker jailed in June of this year as a result of his involvement with the Cum-Ex scheme. In Denmark, authorities have subpoenaed more than 420 companies and individuals in connection with the scandal. The indications are that we can expect to see a number of civil and criminal actions brought against firms and companies across Europe for years to come. How regulatory enforcement efforts unfold over the next few years, and indeed the extent to which they are successful, is certainly one to watch.

4. Cyber risk in financial services

4.1 Introduction

The last two years have seen a significant increase in cyber attacks, particularly ransomware, supply chain attacks and attacks attempting to take advantage of Covid-19. Financial institutions are the target of these attacks just as other sectors are, perhaps even more so given their business, reliance on IT infrastructure to operate, and their interconnected nature.

Having said that, many financial institutions both in the UK and EU have been subject to significant testing in relation to cybersecurity by regulators for a number of years and are subject to more stringent legal and regulatory requirements than many sectors. At the same time, there is a lack of consistency on approach between jurisdictions, with an overlapping patchwork of legislation and guidance from regulators. This can make it difficult for financial institutions to establish a compliance baseline around cyber, and then flex that baseline where necessary in some jurisdictions.

In many EU Member States, and the UK, substantial parts of the financial sector are classified as critical infrastructure. This creates an additional legislative and regulatory overhead, in addition to the usual requirements in relation to data protection and cybercrime. The fact that legislation such as the EU Directive on Network and Information Systems ("NIS Directive") is implemented at national level, with only a certain degree of consistency and without prescriptive standards, makes compliance even more difficult. In the event of a notifiable incident, financial institutions may have reporting obligations under national implementation of the NIS Directive, the EU General Data Protection Regulation ("GDPR"), the revised EU Payment Services Directive ("PSD2"), and potentially also the European Central Bank/Single Supervisory Mechanism, all with different deadlines and thresholds for notification, creating a complex and burdensome matrix of reporting obligations.

This article considers some of the key current cyber risks for financial institutions, the approach of regulators to those risks and mitigating strategies, and upcoming expected legislative changes.

4.2 Supply chain risk

Supply chain cyber risk for businesses, and financial institutions in particular, is not new, with some attacks known from a decade ago. The principle is that, as the defence and response capabilities of high value targets (such a financial institutions) improve, one way to compromise those targets is indirectly, via attacks on third parties whose software or technology those high value targets may use. The additional benefit is that attackers get more value from their attack, as they may be able to infect multiple downstream targets.

The last 18 months have seen a number of high profile supply chain attacks impacting a number of industries. The FCA Cyber Coordination Groups have specifically identified the importance of identifying and managing supply chain risk, noting that "the profile of each third party should be measured and continually assessed to ensure they remain within risk appetite".

Key to understanding and assessing third party supplier risk is understanding what the business use of the third party technology is, what risk that creates for the business, the risk and dependencies of the third party, and how that aligns with the financial institution's risk appetite (both at the time of contracting and over time). This end-to-end understanding requires early engagement with the third party supplier, an open exchange of information, and a willingness by the financial institution to challenge and stress test the answers that they are given. Alignment of security and information management certifications can certainly assist with this process, but should not be viewed as "the answer". They are a helpful stating point but no more.

As the technology stacks of financial institutions have become more complex, considering third party supplier risk is no longer sufficient. In appropriate circumstances, institutions should also consider fourth or even fifth party supplier risk. By the very nature of the fact that such parties are further down the supply chain, and have no contractual nexus with the financial institution, assessing this risk is much more difficult. While regulators will likely take this into account when considering whether appropriate risk assessment was undertaken, and mitigating steps put in place, institutions cannot be blind to this risk.

4.3 Cloud risk

While many fintechs and challenger financial institutions have designed themselves for cloud first, many more traditional financial institutions have been migrating to the cloud for a number of years, and this trend is increasing. This has been recognised by regulators, who recognise the security benefits of a shift to cloud, but also note the risks created (see for example the well-known Final Report on EBA Guidelines on Outsourcing Arrangements, 25 February 2019 and 2017 guidance on the use of cloud service providers). Cloud security is a skillset in itself, and the impact of the skills shortage in cloud security has been consistently recognised as particularly acute, even within the wider cybersecurity skills shortage.

Financial institutions do not, to date, appear to have suffered from many of the more common issues arising from a shift to cloud, such as misconfigured cloud storage servers which can allow easy access to data. However, the complexity of their IT infrastructure, hybrid models and operational resilience and redundancy requirements can create a complex matrix of systems. Understanding how those systems inter-relate, communicate with each other, and who should have access to what (both within and outside the institution's network) is crucial to getting a shift to cloud right.

This involves a deep understanding of the relevant data, infrastructure, products and services, and risks associated with them; a multi-disciplinary approach is essential. Understanding what a move to cloud means for the institution, with its own unique existing systems and technology stack, processes, people, and approach to transformation, allows the business to assess and understand the risks (and benefits) created by that move, and put in place appropriate controls and mitigations.

4.4 COVID-19 and hybrid working models

Supply chain risk and cloud risk both exist on their own. However, changes to working practices and associated changes to technology stacks arising from COVID-19 resulted in digital transformation that might otherwise have taken years happening in only weeks or months.

Sudden shifts to the vast majority of employees working from home drastically changed institution's attack surface and made endpoint management and security immediately more difficult. New technologies were put in place, or existing technologies scaled far beyond their previous use, almost overnight to allow institutions to continue to do business effectively. In our view, this is likely to have stored up significant cyber risk, as audit and risk assessment processes will have been compressed, and sometimes done with a "minimum necessary" approach instead of the usual detailed processes. That may have resulted in excessive mitigations and protections being put in place out of an abundance of caution, causing inefficiency, or alternatively risks may not have been identified or assessed accurately, creating exposure which could be exploited in the future. Now that the immediate COVID-19 transformation rush has diminished, institutions should carefully review risk assessments and mitigations that were done or put in place at the time, and consider in the cold light of day whether they are adequate.

COVID-19 also resulted in cultural change; employees think differently when working from home to in the office, perhaps meaning they are more likely to fall victim to phishing attacks. IT workarounds become more common, and shadow IT is likely to increase. While much of this risk can be mitigated by technological measures, that is not entirely the case. As institutions shift to a longer-term hybrid model, or perhaps returning to the office full time, consideration should be given to whether training and policies remain appropriate relative to either pre-pandemic, or COVID-19, situations.

4.5 The future

There is significant new legislation on the horizon, at least in the EU, which is likely to both increase the cyber regulatory overhead for financial institutions, and increase the scope of those within that regulatory perimeter.

For example, the anticipated Revised Directive on Network and Information Systems (commonly known as the NIS2.0 Directive) will replace the current NIS Directive. The EU Digital Operational Resilience Act has been through several drafts, and will increase the regulatory perimeter for financial services such that some service and technology providers to financial institutions are brought within that perimeter. This is on top of the tens of pieces of legislation, guidance and so on which have been passed or promulgated by regulators in the last few years.

It may be that this new legislation introduces some much needed harmonisation and consistency. However, it is not clear that this will be the case; national implementation will still result in inconsistency, and the Body of European Regulators for Electronic Communications ("BEREC") in May 2021 noted that the holistic approach proposed by NIS2.0 may not always be productive or conducive to competition.

It remains to be seen what the future looks like. What is clear is that cyber regulation in the financial sector has been, and remains, on the increase in the EU, UK, and US (not considered in any detail in this Bulletin). While discussions are ongoing between regulators globally, and there is some move towards increased information sharing and standardisation in some areas, there is much to be done in these areas and until progress is made at a geopolitical level, the complex cyber compliance burden on financial institutions is only likely to increase.

5. A Guide to spotting—and stopping—authorised push payment fraud

5.1 Introduction

For many businesses, the COVID-19 pandemic has caused a squeeze on finances, a reprioritisation of resources, absence of key staff, more home working and pressure on financial and compliance controls. In short, the pandemic has helped create a perfect environment for fraud. One of simplest and most devastating frauds that can be committed against a business is the so-called authorised push payment ("APP") fraud.

5.2 What is authorised push payment fraud?

APP fraud is perpetrated by a fraudster manipulating the trust and confidence of a victim and persuading the victim to make what appear to be authorised payments into accounts ultimately controlled by the fraudster.

The fraudster often masquerades as a senior employee of a supplier or government body, and directs a fictitious email requesting payment or a change in bank details to a junior employee in the target company (often in the accounts or finance function). The method of communication leading to the authorisation of payment tends to be highly convincing, as it aims to replicate or closely mirror a legitimate supplier or other entity's email address, contact name(s) and signature block. The fraudster may have hacked into the email system of the target company and be monitoring when certain emails are sent and received. Alternatively, the fraudster may be working alongside individuals within the target company to obtain the information they need to perpetrate the fraud.

Once the funds are transferred to the fraudster's bank account, the funds are typically immediately dispersed by the fraudster via a series of separate transactions into multiple separate accounts (often located abroad) also controlled by the fraudster, where the funds are then, quickly, withdrawn in cash and further dissipated. Recovering the funds once they have been paid into the fraudster's account is incredibly challenging, but not impossible if steps are taken as soon as the fraud is discovered (see below).

5.3 Rise in authorised push payment fraud during COVID-19

Fraudsters have been adapting their techniques during the COVID-19 pandemic, using increasingly sophisticated schemes to defraud both businesses and individuals.

UK Finance found that, in 2020, the total losses attributable to APP in the UK amounted to a staggering £479 million,[15] with close to 150,000 reported incidents of APP.[16] Over 60% of APP incidents originated online,[17] with the 8,222 impersonation scams recorded amounting to a 94% increase on the previous year.[18]

5.4 An APP case study

One such case the authors were involved in concerned a client based outside of the UK that was subjected to a multi-million dollar APP, perpetrated by an unidentified fraudster masquerading as the client's trading counterparty. The fraudster created email addresses very similar to the ones used by the trading counterparty, set up a bank account with the same name as the trading counter-party, and then directed our client to pay genuine invoices, previously received from the genuine trading counterparty, into the fraudster's bank account. The fraudulent email purported to come from a very senior member of the client's parent company and was directed to a junior member of our client's finance team. The fraudster explained the change in bank account details as being a result of fictional restrictions on UK banks as a result of the COVID-19 pandemic, meaning that payments had to be made to a new bank account (the fraudster's account) on an interim basis.

Once instructed, we immediately notified the banks involved in the transaction and applied for urgent injunctive relief in the English courts to freeze the stolen funds and a disclosure order for information to enable our client to establish whether any and, if so how much, of the stolen funds remained in the fraudster's account, and the location of any accounts into which the stolen funds had been paid.

The entire proceedings took place remotely using online hearings, the first of which took place within hours of the application being made. We believe that, as a result of the hearing taking place online, we were able to obtain the orders our client sought more quickly and cost effectively than would have been the case if an in-person hearing had been required.

We also engaged on behalf of the client with the UK and local criminal authorities and their investigations into this matter. This highlights the importance of needing to consider both civil and criminal law processes in order to secure redress.

As a result of this action, monies in the fraudster's bank account were successfully frozen and recovered by our client.

Most victims of this type of fraud are not so lucky and end up not being able to recover any of the money stolen from them. Victims in such circumstances are left with little recourse against third parties or insurance.

5.5 How to spot APP and how to stop it

Given the current financial predicament in which many businesses find themselves, the increased reliance on technology and the increase in remote working brought about as a result of COVID-19, all businesses, large and small, should be on the lookout for APP-type frauds and ensure they have robust systems in place to help minimise the risk of becoming a victim.

In particular, businesses should consider adopting the following recommended practices:

- A check should be made of the email address from which any payment instructions are received. That address should match exactly the email address from which payment instructions have previously been sent.
- Have a personal contact at your regular suppliers. Always verify details of any amended payment instructions verbally with these contacts before making any payment.
- Ensure all staff, particularly those that are responsible for making payments, are familiar with how APP fraud works, and what signs to look out for.
- Have an approvals process in place which requires the sign-off of payments by more than one member of staff over a certain amount. Ensure that those with the authority to sign-off are in the department responsible for the expenditure.
- Look carefully at each invoice and compare it to previous invoices, particularly the bank account details, wording used and the company logo to check for irregularities.
- When you have paid an invoice, inform the supplier or other trading counterparty of the payment details immediately, including the account to which the payment was made so that any irregularities can be quickly identified.
- Invest in up-to-date cybersecurity technology/software to prevent hacking/malicious attacks against the workforce, which can make it easier for a fraud to be committed.
- Encourage a speak-up culture within the workplace so that, once detected, the fraud can be dealt with expediently.

- Consider removing or limiting certain information, such as testimonials, from company websites and social media channels that could lead fraudsters to know who your regular suppliers and trading counterparties are.
- Every member of the finance/account function (regardless of seniority) should be trained on these systems and controls and should understand that they should treat any request to change payment details of suppliers or other regular service providers with extreme caution.

It is now more important than ever that these systems and controls are implemented and that they remain robust.

5.6 What to do if you suspect a fraud?

If you suspect that you or your business has been the victim of an APP (or any) fraud, it is crucial to act quickly if you are to have any chance of recovering stolen funds. You should immediately do the following:

- Inform all banks involved that the transaction(s) are fraudulent. This is best done over the phone in case email systems have been compromised by the fraudsters.
- Take active steps to check that no other payments have been compromised.
- Notify the legitimate supplier so that they can inform other customers and check for security breaches.
- Seek legal and technical advice on the next steps and any potential action to trace, preserve and recover the stolen funds.

6. US AML developments: US Anti-Money Laundering Act of 2020

6.1 Anti-Money Laundering Act of 2020

The US anti-money laundering ("AML") regulatory framework, which derives its statutory authority from the US Bank Secrecy Act ("BSA") and is reflected in regulations promulgated by the US Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), is slated for a number of significant changes under the US Anti-Money Laundering Act of 2020 ("AMLA"), which became law in the US earlier this year as part of the National Defense Authorization Act for Fiscal Year 2021. AMLA includes the most significant changes to the US AML regime since the enactment of the USA PATRIOT Act of 2001 by directly amending certain provisions of the BSA and requiring FinCEN to take action to modernise its regulations in an effort to address evolving risks to the security of the US financial system.

The primary purposes of AMLA are to: (i) improve coordination and information sharing among the various US agencies and law enforcement bodies charged with administering and enforcing the US AML and countering the financing of terrorism ("CFT") regulatory and statutory framework; (ii) modernise AML/CFT laws to better address emerging money laundering and terrorist financing threats; (iii) encourage technological innovation and the adoption of new technology by financial institutions to deal with these threats more effectively; (iv) reinforce the risk-based approach to AML/CFT regulatory compliance; and (v) discourage the use of anonymous shell companies through the establishment of legal entity beneficial ownership information reporting requirements and a non-public database of such information maintained by FinCEN.

AMLA impacts various types of entities and many of its provisions are applicable to "financial institutions" as defined under the BSA, including banks, broker-dealers, branches and agencies of foreign banks, money services businesses, nonbank lending companies, insurance companies, operators of credit card systems, mutual funds, futures commission merchants, etc. A number of key AMLA provisions are discussed below.

6.2 Corporate Transparency Act

The signature AMLA provision is the Corporate Transparency Act ("CTA"). The CTA establishes a beneficial ownership registry for certain companies formed in the US to be maintained by FinCEN. The absence of such a registry in the US to this point had been viewed by the international community and many US lawmakers as a significant gap in the US AML regulatory framework. Critics argued that the US had become a preferred jurisdiction for establishing corporate vehicles—shell companies, special purpose vehicle, etc.—to facilitate illicit activities by persons, including foreign persons, who were not required to identify themselves. FinCEN has not yet published final rules establishing the beneficial ownership registry, but the statute itself provides a good idea of what the registry will look like and raises a number of issues that are likely to arise in its execution. FinCEN has sought feedback from market participants in regards to a number of these issues in an advance notice of proposed rulemaking published in April 2021.

Not all entities will be required to report beneficial ownership to FinCEN. Although the CTA contains a number of significant exclusions, making clear that the intent of the statute is to discourage the formation of shell companies in the US, the categories of entities not specifically excluded is unclear. Specific exclusions include: (i) public US issuers; (ii) companies that employ more than 20 full-time employees, operate from a physical US office, and have more than $5 million in annual gross sales or receipts; (iii) companies that are in existence for over one year, are not engaged in active business, are not owned directly or indirectly by a foreign person, and do not hold any type of assets; (iv) charitable trusts and charitable organisations; and (vi) pooled investment vehicles. It is not clear whether trusts or partnerships will be required to report beneficial ownership.

The registry will not be public but will be available to US law enforcement as well as foreign law enforcement when requested through established processes for international cooperation between the US and the requesting country, such as a mutual legal assistance treaty or otherwise. Financial institutions that are required under the BSA to maintain an AML compliance program will also have access to the information in the registry provided that they obtain consent from the corporate entity that is the subject of the financial institution's request.

6.3 Clarification of FinCEN's authority to regulate virtual currency businesses

FinCEN has previously issued guidance making it clear that virtual currency businesses that qualify as money transmitters are subject to FinCEN registration requirements for money services businesses.[19] AMLA amends a number of definitions in the BSA to insert the term "value that substitutes for currency" in a number of key definitions that previously referenced only "currency" or "funds."[20] These amendments have the effect of codifying the existing guidance and regulatory provisions and making it clear that FinCEN has the statutory authority to regulate businesses involved in the transfer and exchange of virtual currencies, to include reporting requirements relating to such assets.

FinCEN has begun the rulemaking process to implement such reporting requirements for banks and money services businesses. Under the proposed rule, banks and money services businesses will be required to file value transaction reports for certain virtual currency transactions with a value of greater than $10,000, a requirement that is similar to the Currency Transaction Reports ("CTRs") that banks and other financial institutions have historically been required to file under the BSA, as well as maintain records of certain virtual currency transactions with a value of greater than $3,000, to include counterparty identification information.

6.4 Suspicious activity and currency transaction reporting feedback and modernisation

AMLA requires FinCEN to conduct a formal review within one year of the enactment of the NDAA of reporting requirements for Suspicious Activity Reports ("SARs") and CTRs for the purpose of reducing unnecessarily burdensome regulatory requirements and ensuring that the information provided satisfies the purposes of such reports as described in the BSA.[21] The financial services industry has long criticised the SAR/CTR reporting regime as outdated and not designed to provide law enforcement with useful

investigatory leads for prosecuting laundering and terrorist financing activities. One of the common criticisms is that financial institutions employ significant resources to meet regulatory obligations for the filing of SARs and CTRs that generate a tremendous volume of reports, most of which are not of use to—or even reviewed by—law enforcement. AMLA directs FinCEN to assess such criticisms with a view towards updating the system.

AMLA requires that the FinCEN review must also include an assessment of whether the monetary thresholds for submission of SARs and CTRs are appropriate.[22] Money services businesses are required to file SARs on suspicious transactions that involve, or aggregate, funds in excess of $2,000 (the threshold is $5,000 for banks and other financial institutions). This monetary threshold has not been adjusted since 1996. Similarly, the $10,000 threshold for the filing of CTRs has not been adjusted since 1970 (the year in which the BSA was enacted). Such low thresholds contribute significantly to the "glut" of reports filed with FinCEN on a daily basis, most of which, as noted above, are of little value to law enforcement. A potential outcome of this aspect of the required review is an increase in the monetary reporting threshold, which could reduce the resources deployed by financial institutions to meet the regulatory requirement. Presumably, such resources could be used in other areas of a financial institution's overall AML/CFT compliance program to more effectively address AML/CFT risk. For example, money transmitters could redeploy resources to enhance and calibrate AML/CFT transaction monitoring models or to conduct additional due diligence on high-risk customers.

6.5 Assessment of the employment of financial technology in combatting financial crime

AMLA requires FinCEN to analyse the impact of financial technology on financial crime compliance.[23] The Act requires FinCEN to periodically convene a global AML and financial crime symposium[24] that focuses on how emerging technology can be used more effectively to combat financial crime.[25] Attendees at the symposium are to include senior executives from regulated firms and will be provided the opportunity to demonstrate potential new technologies under development for use in a variety of contexts, including the detection and reporting of suspicious activity.[26]

The recognition of the utility of emerging technologies to regulated entities in meeting regulatory requirements under the BSA is consistent with the Act's formal recognition of a risk-based approach to BSA compliance. While the codification of this risk-based approach is consistent with long-standing guidance from FinCEN and the federal functional regulators for AML/CFT compliance, the amendment to the BSA reflects a recognition that regulated entities should be encouraged to employ technology in a risk-based manner to meet emerging threats. The focus on technology and a risk-based approach to BSA compliance as embodied in the Act is a signal to regulated institutions that supervisors and examiners will be more receptive to the use of non-standard methods that leverage technology when assessing BSA compliance.

6.6 "Keep open" directives safe harbor

AMLA amends the BSA to provide a safe harbor for financial institutions that comply with a "Keep Open" directive from federal law enforcement. Federal law enforcement agencies have historically issued such directives requesting that a financial institution continue to "keep open" an account that may be involved in criminal activity, notwithstanding that doing so may be inconsistent with the institution's obligations under the BSA. FinCEN has previously issued guidance[27] indicating that if a financial institution chooses to maintain the account at the request of law enforcement, the financial institution is required to comply with all BSA recordkeeping and reporting requirements. In most cases, maintaining such an account is inconsistent with a financial institution's internal policies. The amendment to the BSA under the Act provides that a financial institution will not be liable under the BSA for maintaining an account in accordance with a law enforcement directive. The lack of relief from the SAR-filing requirement seems inconsistent with the purpose of a SAR, which is to alert law enforcement to potential suspicious activity. In the circumstance of a "Keep Open" directive, law enforcement is, by definition, already aware.

6.7 Financial inclusion and mitigation of the effects of de-risking

In light of the stringent requirements of the BSA and potential penalties for non-compliance, many financial institutions take a risk-averse approach in the assessment of customer relationships. Such approach often leads to the termination of, or prohibition against, customer relationships that may expose the financial institution to a level of financial crime risk that is not within an institution's conservative risk appetite. For example, there have been well-publicised instances of financial institutions refusing to provide money transmission services to Somalia. Such an approach is reasonable as the compliance burden and regulatory risk associated with maintaining such business (i.e., potential civil or criminal liability) generally outweighs the reward (i.e., profit) associated with the business.

There is a general recognition that such "de-risking," a term that is generally understood to refer to a circumstance where a financial institution terminates a customer relationship in order to avoid the risk associated with the customer rather than manage the risk, has led to the exclusion of certain underserved populations from traditional financial services. In many cases, such populations are forced to obtain financial services in unregulated channels which are often used to facilitate financial crime, such as shadow banking systems and black markets. As part of the required FinCEN review to assess SAR and CTR filing requirements, FinCEN is required to consider the most appropriate means to promote financial inclusion and address the adverse consequences of de-risking certain categories of relationships.[28] Further, the Act requires the Government Accountability Office to conduct a review that will, among other things, identify options for financial institutions that maintain accounts for high-risk categories of clients without compromising the effectiveness of the regulatory AML/CFT requirements.[29] Presumably, the report will provide guidance to financial institutions that will provide for the maintenance of such high-risk relationships in a manner that is consistent with the requirements of the BSA.

7. The *Quincecare* duty of care: Where are we now?

7.1 Introduction

Under the *Quincecare* duty of care owed by banks to customers, a bank must refrain from executing a payment instruction if and for as long as it has been "put on inquiry" by having reasonable grounds for believing that the instruction is an attempt to misappropriate the customer's funds. This forms part of a bank's implied contractual duty to exercise reasonable skill and care in carrying out its customer's instructions.

In practice, the *Quincecare* duty means that banks may sometimes find themselves between a rock and a hard place when it comes to executing instructions for payment. A bank's primary obligation is to promptly execute its customer's instructions in accordance with the customer's mandate, and if the bank fails to do so, it risks a claim for any losses suffered by the customer. However, a bank may be exposed to a negligence claim if it executes instructions in circumstances when it should have refrained from doing so under the *Quincecare* duty.

This section examines some of the key developments emerging from recent cases concerning the *Quincecare* duty and goes on to consider what practical steps banks can take to mitigate potential risks arising from the duty.

7.2 Key developments

7.2.1. The *Quincecare* duty does not extend to genuine payment instructions given by the customer itself

The case of *Philipp v Barclays Bank UK Plc* [2021] EWHC 10 (Comm) confirmed that the *Quincecare* duty will only be engaged where an agent of the customer has attempted to misappropriate the customer's funds. It will not apply where the customer itself has given a genuine payment instruction to the bank, even if that instruction has been fraudulently induced (in *Philipp*, a fraudster had convinced the customer

to instruct her bank to transfer £700,000 from her account in a case of authorised push payment fraud). The High Court found that requiring banks to second-guess the genuine instructions of their customer in the absence of a clearly recognised banking code governing such circumstances would impose an impractical burden on banks.

However, in the case of corporate customers, it is important for banks to remember that the customer is the company itself, even if one individual exercises a dominant influence over the affairs of that company. In *Singularis Holdings Ltd (In Liquidation) v Daiwa Capital Markets Europe Ltd* [2019] UKSC 50, Maan Al Sanea, the sole shareholder and chairman of Singularis (which had been set up to manage Al Sanea's personal assets) instructed Daiwa to make a number of large payments from Singularis's accounts. Through these payments, Al Sanea had in fact been misappropriating the assets of Singularis. Despite his control over the company, the Supreme Court found that Al Sanea's fraud could not be attributed to Singularis: his actions were that of an agent acting on behalf of the company and the *Quincecare* duty applied in the usual way.

7.2.2 The *Quincecare* duty is owed to the bank's customer, not the customer's creditors

Allegations of a breach of the *Quincecare* duty may often arise in circumstances where the customer, by virtue of the fraud perpetrated against it, is technically insolvent at the time of the alleged breach. However, the case of *Stanford International Bank (SIB) v HSBC Bank Plc* [2021] EWCA Civ 535 highlights that while insolvency may affect the duties of the customer's directors (who must now act in the best interests of the customer's creditors, rather than its shareholders) the *Quincecare* duty continues to be owed to the customer itself, and the usual principles of assessing recoverable loss suffered by the customer continue to apply.

In *Stanford*, SIB's liquidators alleged that HSBC had failed to spot warning signs that SIB was being run as a Ponzi scheme by its beneficial owner, with the effect that £118.5 million had been paid out of SIB's accounts with HSBC that would have otherwise been available to distribute to creditors in the insolvency process. However, all but one of the payments made out of the accounts had either discharged SIB's liabilities owed to other investors or been paid to SIB's accounts at other banks: in other words, the net effect on SIB's balance sheet was zero. The Court of Appeal held that in those circumstances, SIB had suffered no recoverable loss. It made no difference that SIB was left with fewer assets to distribute to its creditors as a result of the payments made out of the accounts. That was a loss suffered by SIB's creditors, rather than SIB itself, and HSBC owed no duty to those creditors.

7.2.3 It may be possible to contract out of the *Quincecare* duty … but boilerplate clauses won't be sufficient

In *JP Morgan Chase v Federal Republic of Nigeria* [2019] EWCA Civ 1641, JP Morgan argued that the *Quincecare* duty was excluded (or never arose in the first place) because of the operation of various provisions in the contract between the parties. In particular, the bank sought to rely on an entire agreement clause, an exemption clause relieving the bank from liability when it acted on what it believed in good faith to be the instructions of its customer, an indemnity in respect of all losses caused by the bank following instructions by which the bank was contractually authorised to act, and various other provisions which it said were inconsistent with the *Quincecare* duty arising.

However, the Court of Appeal held that these provisions did not exclude the *Quincecare* duty: the duty bestowed a valuable contractual right on the customer, and clear unequivocal words were therefore needed to exclude such a right. Nevertheless, the Court of Appeal's judgment in this case should provide some encouragement for banks. The Court of Appeal expressly acknowledged that it would not be impossible for the bank and its customer to contractually exclude liability for breach of the *Quincecare* duty. However, depending on the circumstances, such an exclusion may be subject to challenge under general contractual principles or on the basis that it contravenes the Unfair Contract Terms Act 1977.

7.3 What should banks be doing to mitigate the risk of a *Quincecare* breach?

(1) **Tighten contractual terms**. Banks should review their customer contracts to ensure that they provide protection against a *Quincecare* claim. In particular, provisions relating to the payment instruction process should be carefully considered, for example, should a second signatory from the customer be required for high value payment instructions to protect against the risk of a rogue agent? Banks may also wish to attempt to carve out liability for the *Quincecare* duty with clear unequivocal language in customer contracts, although as above, this may be subject to challenge.

(2) **Ensure appropriate risk-monitoring systems are in place**. Systems and processes such as adverse news coverage alerts and suspicious transaction monitoring may act as an early warning system for potential fraud in respect of an account which could give rise to a *Quincecare* risk. Banks that operate global businesses should try to ensure that such systems work in a joined-up way; for example, will a regulatory enquiry about a customer in one jurisdiction be flagged up on accounts belonging to an affiliate of that customer in a different jurisdiction?

(3) **Communicate with front office teams about managing fraud risk**. Even best-in-class compliance systems will fall short if front office staff fail to act on the red flags that are generated by those systems (and a failure to act on known red flags may be even more damaging in a negligence action than failing to spot the risk at all). Banks should consider rolling out mandatory training to relationship managers and other front office employees on how to spot potentially fraudulent instructions given by a customer's agent, and what to do if red flags are identified. In particular, front office teams should be made aware that liability may arise under the *Quincecare* duty even if they receive authorised payment instructions from the customer's agent.

(4) **Put in place processes to ensure that red flags are acted upon ...** Although the appropriate action upon becoming aware of red flags in connection with a customer's account will vary on a case-by-case basis, banks should adopt a clear process for dealing with this scenario, which should include assigning responsibilities for following up on red flags and documenting key decisions.

(5) **... but beware of tipping off the fraudster**. Circumstances which engage the *Quincecare* duty will often also necessitate making a Suspicious Activity Report to the National Crime Agency. Banks should ensure that they adopt a joined-up strategy to handle both workstreams. In particular, banks should consider whether their potential liability under the Proceeds of Crime Act (especially under the tipping off offence) places limits on the enquiries that can reasonably be made of the customer pursuant to the *Quincecare* duty.

Endnotes

1 *Lennard v Asiatic Petroleum* [1915] A.C. 705.
2 Lisa Osofsky's comments, 23 October 2020 at h*ttps://www.sfo.gov.uk/2020/10/23/serious-fraud-office-releases-guidance-on-deferred-prosecution-agreements/*.
3 Code for Crown Prosecutors, para.4.6.
4 Code for Crown Prosecutors, paras 5.1–5.11.
5 *https://www.sfo.gov.uk/download/amec-foster-wheeler-energy-limited-deferred-prosecution-agreement-judgment/*, para.12.
6 *https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/*.
7 *https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/*.
8 *https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/deferred-prosecution-agreements-2/?preview=true#_ftn4*.
9 *https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/#_ftnref2* (see *R v Derby Magistrates Court ex part B* [1995] 4 All E.R. 526).
10 *https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/deferred-prosecution-agreements-2/*.
11 *https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/deferred-prosecution-agreements-2/*.
12 *https://www.lawcom.gov.uk/law-commission-seek-views-on-corporate-criminal-liability/*.
13 *https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/06/Corporate-Criminal-Liability-Discussion-Paper.pdf* at p.35.
14 *https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/06/Corporate-Criminal-Liability-Discussion-Paper.pdf* at para.4.11
15 *https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf* at p.6.
16 *https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf* at p.6.
17 *https://www.ukfinance.org.uk/press/press-releases/over-two-thirds-of-all-app-scams-start-online%E2%80%93new-uk-finance-analysis*.
18 *https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2020-FINAL.pdf* at p.6.
19 See Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, May 2019, at *https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.*
20 AMLA, §6102(d).
21 AMLA, §6204.
22 AMLA, §6205.
23 AMLA, §6210.
24 The timing of the first symposium is not clear, although the language of the statute requires FinCEN to "periodically convene" such a symposium, suggesting that the FinCEN will do this on perhaps an annual or bi-annual basis.
25 AMLA, §6211.
26 AMLA, §6211(c) and §6211(d).
27 See Requests by Law Enforcement for Financial Institutions to Maintain Accounts, June 2007, at *https://www.fincen.gov/resources/statutes-regulations/guidance/requests-law-enforcement-financial-institutions-maintain*.
28 AMLA, §6204(b)(2)(F).
29 AMLA, §6215.

COMPLIANCE OFFICER BULLETIN

COMPLIANCE OFFICER BULLETIN

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

For over 18 years, Compliance Officer Bulletin has been dedicated not only to aiding compliance officers to keep up to date with an unending series of changes to the UK regulatory regime, but also to providing unrivalled commentary and analysis on how FCA and PRA regulations impact on them and their business.

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

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