SHEARMAN & STERLING

UK BUSINESS CRIME REVIEW 2020

25 FEBRUARY 2020

Shearman

CONTENTS

UK BUSINESS CRIME REVIEW 2020

INTRODUCTION

This is the first edition of *U.K. Business Crime Review*—an annual publication focused on the outcomes, trends and developments over the past 12 months that are likely to be of interest to businesses operating in the United Kingdom.

Whilst this publication primarily focuses on the introduction and use of criminal sanctions in the business crime space, we also consider key regulatory developments that are likely to be of interest to those managing financial crime risks within businesses.

Readers interested in gaining a global perspective on the topics covered should also look to other Shearman & Sterling resources, such as the *FCPA Digest*, *Sanctions Round Up* and our financial regulation blog at finreg.shearman.com.

OVERVIEW

In the first section of this publication, we focus on the actions of those bodies operating at a national level, whose work is likely to be of most interest to readers—the Serious Fraud Office (SFO), the Financial Conduct Authority (FCA), the National Crime Agency (NCA), Her Majesty's Revenue & Customs (HMRC) and the Office of Financial Sanctions Implementation (OFSI).

In the second section of this publication, we examine key outcomes or developments in a little more detail. In this edition, we focus on Airbus SE avoiding prosecution by reaching a €3.6 billion settlement with the authorities in the U.K., France and the U.S.; the implementation of the EU's Fifth Money Laundering Directive; and the cooperation mechanisms in place in relation to criminal matters following the U.K.'s withdrawal from the European Union.

In the final section, we consider other matters that are likely to be of interest to readers, including recent enforcement action taken by the Information Commissioner's Office; the conclusion of a bilateral data access agreement between the U.K. and the U.S.; the U.K.'s indication that it will not implement the EU's Whistleblowing Directive; and the removal of the ban on TV recording in Crown Courts in England and Wales.

KEY LEGISLATIVE DEVELOPMENTS

The political landscape over the past 12 months has been dominated by the U.K.'s withdrawal from the European Union, which took place at 23:00 GMT on 31 January 2020. This meant that somewhat unusually in recent years, 2019 did not see the enactment of a flagship statute that significantly altered the business crime landscape in the U.K. That said, there were three legislative developments that we consider to merit consideration in this publication.

The first is the enactment of the European Union (Withdrawal Agreement) Act 2020, which gives legal effect in the U.K. to the Withdrawal Agreement concluded with the EU. Of particular relevance to the subject matter of this publication is the fact that under the Withdrawal Agreement, the U.K. will continue to enjoy the many mechanisms that allow cooperation in criminal matters across the EU until the conclusion of the implementation or transition period, which is currently scheduled to come to an end on 31 December 2020.

The second is the enactment of the Crime (Overseas Production Orders) Act 2019, which permits a U.K. court to issue an order directly against a communication service provider located in another country, requiring it to produce electronic data (such as e-mails and text messages), if the U.K. has entered into an international cooperation agreement with the relevant country. Such an agreement was concluded between the U.K. and the U.S. on 3 October 2019.

The third is the introduction of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, which implemented the EU's Fifth Money Laundering Directive by amending the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The amendments came into force on 10 January 2020.

KEY ENFORCEMENT OUTCOMES

Without a doubt, the Deferred Prosecution Agreement concluded between the SFO and Airbus SE in January 2020 is the standout enforcement outcome from the past twelve months. Under the agreement, Airbus SE must pay a financial penalty and costs totalling almost €1 billion as part of a €3.6 billion settlement reached with the U.K., French and U.S. authorities to avoid prosecution. This record-breaking penalty is the largest ever imposed by a U.K. criminal court and is double the total of all fines paid in respect of criminal conduct in England and Wales in the whole of 2018.

The other outcome of note is the £102 million regulatory penalty imposed against Standard Chartered Bank by the FCA in April 2019 for shortcomings in the Bank's anti-money laundering controls relating to customer due

diligence and ongoing monitoring. The penalty is the second largest imposed by the FCA against a firm for AML failings.

KEY TRENDS

Both outcomes detailed above highlight the continued appetite of U.K. enforcement agencies to pursue corporate failures to properly implement, monitor and enforce adequate policies and procedures to prevent financial crime.

Of course, a cynic may say that large companies keen to avoid prosecution or severe regulatory action are viewed by some as soft targets who are only too willing to pay significant financial penalties to escape such a fate. The end result being viewed as a "win-win" situation for all involved—the chance for companies to put matters behind them and turn over a new leaf; an opportunity for enforcement agencies to bask in the glory of securing a headline-grabbing result; and a sizeable injection of capital into the coffers of Her Majesty's Treasury.

Whether such a view is accurate or not, there appears to be no indication that the U.K. Government, or law enforcement agencies, prosecuting bodies or regulators, will be charting a different course in the near future. Indeed, many are calling for the extension of "failure to prevent" offences (similar to those under the Bribery Act 2010 in relation to bribery and corruption, and the Criminal Finances Act 2017 in relation to the facilitation of tax evasion) in an effort to tackle other forms of serious economic crime.

Some commentators believe that this is all part of a growing trend to shift the burden of tackling serious economic crime to the private sector following the realization that those tasked with enforcing the rules will never have sufficient resources to confront the many challenges they face in this area. The U.K. Government is not shy about its ambitions—building an effective public-private partnership lies at the heart of the Economic Crime Plan for 2019 to 2022, which was published by HM Treasury and the Home Office in July 2019.

In addition to punishing corporations for failing to prevent bribery and corruption or the facilitation of tax evasion, or for having inadequate systems in place to prevent money laundering and terrorist financing, recent decisions also indicate that businesses are likely to be the subject of regulatory or civil enforcement action if their acts or omissions create situations that may be exploited by criminals. As a result, businesses must ensure that they properly process and store personal data, and that they have adequate mechanisms in place to limit the risks of their IT systems being compromised, leading to information being stolen and misused. As the FCA has publicly announced, examining firms' "operational resilience" will be a key priority in 2020.

Taking all of these matters into account, readers may conclude that it has never been more important for businesses operating in the U.K. to devote adequate expertise and resources to implementing, monitoring and enforcing the mechanisms necessary to avoid falling foul of the ever-increasing legal and regulatory framework under which they now operate and, more importantly, their being used to facilitate serious economic crime.

ENFORCEMENT ROUND-UP

- SERIOUS FRAUD OFFICE
- FINANCIAL CONDUCT AUTHORITY
- NATIONAL CRIME AGENCY
- HER MAJESTY'S REVENUE & CUSTOMS
- OFFICE OF FINANCIAL SANCTIONS IMPLEMENTATION

SERIOUS FRAUD OFFICE

As readers will be aware, the Serious Fraud Office (SFO) is tasked with tackling "the top level of serious or complex fraud, bribery and corruption." It is unusual in the U.K. because it both investigates and prosecutes its cases through multi-disciplinary teams, and has done since it was established in 1988. However, while its operating model has remained largely the same, the types of cases it tackles has not. The SFO is therefore at the forefront in finding new ways to obtain, sift and review vast quantities of data. It was also one of the first agencies to embrace the use of artificial intelligence to assist in document analysis, which it trialed during the investigation against Rolls-Royce plc. It will be interesting to see how the use of this technology plays out as contested cases reach the courts.

2019 continued to be a busy time for the SFO with several prosecutions reaching a conclusion and a number of new investigations announced. While results over the past 12 months could be described as "mixed," the SFO's fortunes improved significantly on 31 January 2020 when Dame Victoria Sharp, the President of the Queen's Bench Division of the High Court, approved the Deferred Prosecution Agreement (DPA) against Airbus SE. Under the agreement, Airbus SE must pay a financial penalty and costs amounting to almost €1 billion. This record-breaking settlement is considered later in the *In-Depth* section of this publication.

2019 also saw the arrival of Sara Lawson QC following her appointment as General Counsel. Prior to her taking up the position, Ms. Lawson QC specialized in prosecuting criminal and regulatory cases on behalf of government and quasi-government bodies, including the SFO.

COOPERATION

"Cooperation" seems to be the buzzword at the SFO at the moment. Lisa Osofsky, the SFO's Director, used her speech at the Cambridge Symposium in September 2019 to stress again the importance of cooperation between law enforcement bodies both in the U.K. and overseas. She also used her speech to emphasize the importance of the private sector "cooperating" in preventing crime, and specifically bribery, from occurring in the first place. However, it is the SFO's updated guidance on corporate cooperation and Ms. Osofsky's comments concerning the cooperation of individuals believed to have engaged in criminality that has attracted the most attention in recent months.

CORPORATE COOPERATION

In August 2019, the SFO updated its guidance on corporate cooperation by publishing the relevant section of its Operational Handbook. Although the Handbook is for "internal guidance only," it is commonly made available (either in full or with redactions) "in the interests of transparency." It is intended to supplement the Guidance on Corporate Prosecutions and the DPA Code of Practice.

Unsurprisingly, the guidance highlights the benefits of organizations cooperating with the SFO to allow it "more quickly and reliably to understand the facts, obtain admissible evidence, and progress an investigation to the stage where the prosecutor can apply the law to the facts."

Cooperation is defined as "providing assistance to the SFO that goes above and beyond what the law requires." The SFO asserts that "many legal advisers well understand the type of conduct that constitutes true cooperation" and observes that "this will be reflected in the nature and tone of the interaction between a genuinely co-operative organisation, its legal advisers and the SFO."

In short, the SFO believes everyone will be able to recognize cooperation when they see it. However, in an effort to assist, the SFO sets out a non-exhaustive list of eleven "good general practices." Many of the practices identified are to be expected, such as preserving material, ensuring digital integrity, and obtaining and providing material promptly. However, the SFO's approach to material over which legal professional privilege is asserted is raising a few eyebrows in London and beyond.

If documents are withheld, the SFO expects to be promptly provided with a schedule of such documents, including the basis for asserting privilege. In addition, if an organization claims privilege, "it will be expected to provide certification by independent counsel that the material in question is privileged." Later in the guidance, the SFO states that "if an organisation decides to assert legal privilege over relevant material (such as first accounts, internal investigation interviews or other documents), the SFO may challenge that assertion where it considers it necessary or appropriate to do so."

Therefore, in this area at least, the guidance is relatively clear—without certification from independent counsel, the SFO is unlikely to accept any assertions as to privilege made by an organization and, even then, the

SFO may seek to challenge any assertion. Such a stance can only have been adopted for two reasons. First, because the SFO is of the view that the legal principles relating to privilege are being routinely misapplied by organizations or, second, because it believes organizations are using privilege as a device to hide behind.

The stance adopted by the SFO is interesting because, under section 2 of the Criminal Justice Act 1987—the legislative provision from which the SFO derives its principal powers of investigation—it is precluded from requiring the disclosure or production of any document over which legal professional privilege can properly be asserted. It is therefore not unreasonable to conclude that the SFO's assessment of the level of cooperation provided may depend, at least in part, on an organization's willingness to provide the SFO with access to material that it would otherwise be unable to obtain. Perhaps this is what the SFO means by going "above and beyond what the law requires."

In contrast, the Principles of Federal Prosecution of Business Organizations issued by the U.S. Department of Justice (DoJ) state:

Eligibility for cooperation credit is not predicated upon the waiver of attorney-client privilege or work product protection. Instead, the sort of cooperation that is most valuable to resolving allegations of misconduct by a corporation and its officers, directors, employees, or agents is disclosure of the relevant facts concerning such misconduct. In this regard, the analysis parallels that for a non-corporate defendant, where cooperation typically requires disclosure of relevant factual knowledge and not of discussions between an individual and his attorneys.

The thinking behind the approach taken by the DOJ is a sensible one—it expects to be provided with the relevant facts regardless of the professions of those used to gather information during the course of a fact-finding exercise or internal investigation. Such an approach ensures that no corporation is at an advantage or disadvantage by using lawyers to gather information when it comes to assessing eligibility for cooperation credit.

Of course, you can hardly blame the SFO for trying to encourage organizations to waive privilege at an early stage, given the difficulties it has encountered in relation to such matters in recent years (see *SFO v ENRC* [2018] EWCA Civ 2006, for example). In the absence of cooperation from an organization, the thorny issue of privilege will often cause significant delay to the progress of an investigation and is almost certain to require the deployment of costly resources. As was demonstrated in *Regina (on the application of AL) v SFO* [2018] EWHC 856 (Admin), an organization's withholding of documents on grounds of privilege may also complicate the prosecution of individuals connected with that organization in later proceedings. In that case, although the Administrative Court upheld the decisions made by the Crown Court Judge, the SFO was admonished for failing to challenge an organization's assertion of privilege and its withholding of interview notes from an internal investigation concerning the company's executives, who were allegedly involved in the bribery scheme at-issue.

The SFO concludes its guidance by stating that "an organisation that does not waive privilege and provide witness accounts does not attain the corresponding factor against prosecution that is found in the DPA Code but will not be penalised by the SFO." The latter may be strictly true, but if an organization that refuses to waive privilege is likely to find it far more difficult to achieve eligibility for a DPA, it is going to feel an awful lot like it is being punished for asserting its legal rights. Surely an approach more in line with that adopted by the DOJ is more appropriate in the circumstances. After all, if an organization is willing to provide the SFO with all relevant facts and goes out of its way to do so, why should that not amount to "true cooperation" merely because it wishes to maintain a genuine claim of privilege over some material?

What remains to be seen is whether an organization must adhere to all 11 "good general practices" to be eligible for a DPA. We envisage that adherence to most of the practices will prove to be sufficient in most cases, as long as any departure from them can be justified in the circumstances.

COOPERATING SUSPECTS

In April 2019, Ms. Osofsky hit the headlines following comments made during an interview with the *Evening Standard* in which she stated that she planned to tell offenders: "you can spend 20 years in jail for what you did or wear a wire and work with us."

In October 2019, during an address at the American Bar Association's Eighth Annual White Collar Crime Institute in London, she again turned to the topic. Ms. Osofsky said:

Even if I don't have all the powers to wire someone up, we do work with partners who actually may have those abilities to do something similar... We can work with either [National Crime Agency] partners or policing partners or others if we've got an investigation that seems to merit that sort of approach.

The SFO regularly works with the National Crime Agency (NCA), police forces and others during investigations, so while the SFO may lack the operational expertise and experience to "wire up" a cooperating suspect, there is no legal or practical impediment to the organization pursuing such a course. However, Ms. Osofsky may have failed to fully appreciate four key differences between the U.S. and U.K. legal systems.

First, even those convicted after trial for white collar offenses rarely receive prison sentences in excess of ten years. In addition, offenders will usually serve less than half of any sentence imposed and the vast majority of that time will be spent in a low-security or "open" prison. In those circumstances, the incentives for suspects to cooperate may be low, while the long-term risks to their safety and security remain high.

Second, in the U.K., it is very unusual for a cooperating suspect to be rewarded with immunity from prosecution, even though the Attorney General is able to authorize such a course. In most cases, a cooperating suspect or defendant will receive additional credit towards any sentence imposed. As the starting point for any sentence following a plea is already likely to be relatively low, any additional credit is unlikely to make any significant difference.

Third, anecdotal evidence appears to suggest that both judges and juries view the evidence of cooperating suspects and defendants with a significant degree of skepticism, and the use of such witnesses may not significantly increase the chances of securing a conviction. As a result, investigators and prosecutors tend to embark on such a course only when evidence cannot be gathered by alternative methods or when pursuing those methods would lead to significant delay.

Fourth, while a cooperating suspect can be used to obtain more direct (and convincing) evidence through the use of wires and recording devices, such tactics are normally used to catch suspected offenders "in the act." In many investigations, the SFO is examining events that have happened some time ago and not a continuing course of conduct. In such circumstances, persuading a suspect to wear a wire may be of little evidential value. That said, a cooperating suspect could still be of value in helping the SFO identify relevant evidence and the key players in any alleged wrongdoing.

EVALUATING A COMPLIANCE PROGRAM

In January 2020, the SFO also updated its guidance on evaluating compliance programs by publishing the relevant section of its Operational Handbook.

The guidance highlights that when investigating any organization, the SFO will need to assess the effectiveness of the organization's compliance program. Such an assessment will inform decisions as to:

- whether an organization may have an "adequate procedures" defense under section 7 of the Bribery Act 2010;
- whether a prosecution is in the public interest;
- whether an organization should be invited to enter into DPA negotiations and, if so, what conditions should be attached to any DPA; and
- the sentence to be imposed in the event of conviction.

The SFO stresses that the key feature of any program is that it needs to be effective and not simply "a paper exercise." It must work for the organization in question, taking into account the field in which that organization operates, and be proportionate, risk-based and regularly reviewed.

As part of any assessment, the SFO will consider the compliance program in existence at the time of any alleged wrongdoing and at the time any assessment is being carried out. The SFO will also take into account any changes that may be made to a compliance program going forward. An organization who has adopted a genuinely proactive approach to implementing remedial actions is far more likely to avoid immediate prosecution and may, in some circumstances, even avoid being the subject of a DPA.

The SFO's guidance also draws on the six principles identified in the statutory guidance published by the Ministry of Justice in 2011, following the enactment of the Bribery Act 2010. The principles will be familiar to many readers. In short, they recommend that organizations seeking to put in place "adequate procedures":

- adopt proportionate procedures;
- secure a "top level commitment" from senior management;
- carry out risk assessments;
- conduct due diligence;
- communicate policies and procedures, and provide appropriate training for staff; and
- monitor and review policies and procedures on a periodic basis.

As the SFO recognizes, the guidance relates to organizations of different sizes, operating in different sectors. It is, therefore, not designed to be prescriptive. However, it does provide organizations with a clear indication of the matters that the SFO will be taking into

account in assessing the effectiveness of an organization's compliance program and, in turn, whether action ought to be taken against it.

SECTION TWO INTERVIEWS

In June 2019, the SFO re-issued its guidance in relation to interviews under section 2 of the Criminal Justice Act 1987. Such interviews are used by the SFO to gain information from individuals who are not suspects in an investigation. A person who fails, without reasonable excuse, to provide answers when questioned may be imprisoned for up to two years and/or fined.

The re-issued guidance follows the High Court's decision in *Regina (on the application of Lord) v SFO* [2015] EWHC 865 Admin, in which the Court confirmed that an individual being interviewed in accordance with the section 2 power is not entitled, as of right, to have a lawyer present and that the SFO, acting reasonably and properly in all the circumstances, is entitled to refuse to permit a lawyer to be present if it considers that such a course might prejudice an investigation. The guidance is therefore intended to set out the circumstances in which the SFO will permit a lawyer to attend and the "ground rules" that will apply.

The SFO states that "a particular lawyer will be allowed to attend [an] interview if the SFO believes it likely they will assist the purpose of the interview and/or investigation, or that they will provide essential assistance to the interviewee by way of legal advice or pastoral support." Anyone wishing to be accompanied by a lawyer is required to set out in writing, in advance, how the presence of a particular lawyer will meet those objectives. If the attendance of a particular lawyer is likely to lead to delay, the SFO states that their attendance is likely to be refused.

In addition, the lawyer who wishes to attend must provide written undertakings that:

- the firm does not represent any other legal person or organization who is a suspect in the investigation;
- all pre-disclosure documents and documents disclosed during the interview will be kept confidential;
- relevant documents will not be provided to or discussed with anyone without the written authority of the SFO;
- relevant documents will not be copied;
- all relevant documents will be provided securely until returned to the SFO at the conclusion of the interview;
- the interview will not be transcribed or recorded, although a note may be taken; and
- the content of the interview will not be disclosed or discussed with anyone without the written authority of the SFO.

As readers will readily appreciate, the undertakings sought by the SFO can create significant practical difficulties and may, in some instances, conflict with a lawyer's professional obligations to their client. What remains to be seen is how rigidly the SFO will stick to its pre-interview requirements.

Anecdotal evidence suggests that some SFO lawyers are certainly willing to show greater flexibility than the guidance would suggest. That may be as a result of a realization that, in almost all circumstances, it will be in the SFO's interests, as well as the person being interviewed, for a lawyer to be in attendance. After all, the person being interviewed is a potential witness whose evidence may be key in securing a conviction at a later date. Leaving interviewees on their own to fend for themselves is likely to have a detrimental effect on the quality of their evidence and may prove counter-productive in the long run.

Of course, no-one can criticize the SFO for wanting to maintain the integrity of its investigations, but surely any guidance issued needs to be capable of being followed in a fair and consistent manner. Ms. Osofsky is quoted as saying that "smart people" will find a way to deal with the SFO's requests, but if applying what should be relatively straightforward guidance requires a significant degree of legal ingenuity, it may be time to reconsider the guidance.

SIGNIFICANT OUTCOMES

In January 2019, the SFO was able to publish, in full, the DPA reached with Tesco Stores Ltd in April 2017 following the collapse of the trial against former senior executives for their alleged role in the financial reporting scandal. All were acquitted. Under the settlement, Tesco Stores Ltd was ordered to pay a financial penalty of almost £129 million and more than £3 million in costs to avoid prosecution.

In February 2019, the SFO announced the conclusion of its long running case against Rolls-Royce plc which resulted in a DPA with the company and one of its subsidiaries in respect of bribery and corruption to win business in Indonesia, Thailand, India, Russia, Nigeria, China and Malaysia. Under the settlement, it was ordered to pay £497.25 million. The SFO did not charge any individuals in connection with the investigation.

In the same month, the SFO also announced the closure of its long running bribery investigation concerning GlaxoSmithKline (GSK), which focused on commercial

practices by the company, its subsidiaries and associated persons. The SFO did not charge GSK or any individuals in connection with the case.

The SFO's ongoing investigation into Petrofac Limited and its subsidiaries continues. In connection with that investigation, on 6 February 2019, David Lufkin, a British national, and previously Global Head of Sales for Petrofac International Limited, pleaded guilty to eleven counts of bribery. These offenses relate to the making of corrupt offers to influence (ultimately unsuccessfully) the award of contracts to Petrofac worth in excess of $730 million in Iraq and in excess of $3.5 billion in Saudi Arabia.

In March 2019, the SFO secured the forfeiture of over £1.5 million from convicted fraudster Nisar Afzal. This was said to be one of the largest seizures of its kind in the U.K. and was the SFO's first use of the power introduced by the Criminal Finances Act 2017. The forfeited money came from the sale of two properties in Birmingham, which Mr. Afzal originally bought with the funds from a series of long-term frauds. He fled to Pakistan in the mid-2000s. His brother, Saghir Afzal, was convicted for his role in a series of mortgage frauds and sentenced to 13 years' imprisonment in 2011.

In May 2019, the SFO commenced criminal proceedings against Anna Machkevitch, a director of London-based ALM Services U.K. and the Machkevitch Foundation, for failing to produce documents to the SFO as part of its ongoing investigation against ENRC. In November 2019, Ms. Machkevitch failed in her attempts to halt the prosecution by bringing an application for judicial review of the SFO's decision to commence the prosecution against her. In refusing her application, Mr. Justice Supperstone stated that the decision was neither disproportionate, unreasonable or "wholly out of the ordinary." Ms. Machkevitch stood trial at Hendon Magistrates' Court in January 2020 and was convicted. She was fined £800 and ordered to pay the SFO's costs in full. She is not a suspect in the SFO's investigation against ENRC.

In June 2019, FH Bertling Ltd, a freight forwarding company, was fined £850,000 for implementing a "planned and systematic" bribery scheme designed to secure $20 million worth of shipping contracts in connection with an oil project in Angola. At the time the company was sentenced, several employees had already received suspended terms of imprisonment for their involvement in the scheme or another that centered on oil exploration in the North Sea.

Also in June, Carole Ann Hodson was sentenced to two years' imprisonment for her part in a scheme that saw almost £300,000 paid in bribes in order to allow ALCA Fasteners Ltd, a company she owned at the time, to win contracts worth around £12 million. A confiscation order in the sum of £4,494,541 was made against her, and she was ordered to pay costs of £478,351. Ms. Hodson was also disqualified from acting as a company director for seven years.

In July 2019, the last scheduled trial arising from the SFO's investigation into EURIBOR manipulation came to an end. Four senior ex-bankers have been convicted for their part in the conspiracy and received sentences ranging from four to eight years' imprisonment. However, it should also be noted that a number of individuals who faced prosecution were acquitted.

Also in July 2019, three former executives of Sarclad Limited, a Sheffield-based steel components company, were acquitted following a trial. The SFO alleged that Michael Sorby, Adrian Leek, and David Justice struck twenty-seven corrupt agreements to secure contracts that the company would not otherwise have obtained. The case was another example of the SFO concluding a DPA against a company, but being unable to secure convictions against individuals for their alleged roles in the criminal activity.

In the same month, Basil Al Jarah pleaded guilty to charges arising from the SFO's investigation into the activities of Unaoil, its employees and its agents in Iraq. He will be sentenced following the conclusion of the trial against three other individuals – Ziad Akle, Paul Bond and Stephen Whiteley—which began at Southwark Crown Court in January 2020. The SFO has not brought any charges against the company. Other individuals have faced prosecution in the U.S.

Also in July, the DPA against Serco Geografix Ltd (Serco) was approved by Mr. Justice William Davis. Under the agreement, Serco agreed to pay a financial penalty of £19.2 million and costs of £3.7 million in order to avoid prosecution for fraud and false accounting arising from its provision of electronic monitoring services to the U.K.'s Ministry of Justice. In December 2019, the SFO charged two individuals with fraud and false accounting in relation to this investigation.

In October 2019, the SFO announced the closure of its investigation into LIBOR manipulation. Prosecutions have been brought against a total of 13 individuals. However, once again, more individuals have been acquitted than convicted.

Also in October 2019, the SFO announced that it had secured a £118,000 uplift in the confiscation order made against convicted fraudster Nicholas Levene, who was sentenced to 13-years' imprisonment in 2012. At the time that the original confiscation order was made in 2013,

Mr. Levene had been declared bankrupt. It was therefore agreed that his available assets totaled just £1. However, in February 2019, the SFO obtained a restraint order under the Proceeds of Crime Act 2002, freezing Mr. Levene's self-invested personal pension to which he would gain access on his 55th birthday. When he reached that milestone, the value of the pension plan became an "available asset," prompting an application under section 22 of the 2002 Act, which allows prosecutors to seek an increase in a defendant's confiscation order if his circumstances change. This example highlights that prosecutors continue to monitor the financial circumstances of convicted persons many years after a prosecution has come to an end.

In November 2019, the long-running criminal proceedings against two Alstom subsidiaries and several individuals concluded with Alstom Network U.K. Ltd being fined £15 million and ordered to pay £1.4 million in costs. This strand of the investigation centered upon contracts to supply trams in Tunisia. While the SFO's investigation led to convictions against two Alstom subsidiaries and three individuals, the prosecutions brought also resulted in a number of acquittals. Several commentators are questioning whether the outcomes merited the time and resources expended on this investigation.

In November 2019, the European Bank for Reconstruction and Development (EBRD) imposed a six-year term of debarment on GE Power Sweden AB following an investigation in collaboration with the SFO. The investigation found that, from as early as 2002, representatives of Alstom Power Sweden AB, a predecessor company to GE Power Sweden, had conspired with another Alstom entity to manipulate the technical specifications for works carried out at a Lithuanian power plant by making payments to Lithuanian government officials. The project was financed by donor funds administered by the EBRD. The debarment, which began on 27 November 2019, is the longest to have been imposed by the Bank. EBRD's Office of the Chief Compliance Officer stated it will also submit debarment of GE Power Sweden AB to the World Bank, the African Development Bank, the Asian Development Bank and the Inter-American Development Bank.

In December 2019, following the acquittal of Cansun Güralp, Andrew Bell and Natalie Pearce after a trial, the SFO announced that it had concluded a DPA with Güralp Systems Ltd in October 2019. The company, which produces equipment and data systems for seismological research and similar applications, accepted that the charges of conspiracy to make corrupt payments and failing to prevent bribery by its employees between 2002 and 2015 were made out, and agreed to pay a total of £2,069,861 by way of disgorgement of profits. The DPA also requires the company to cooperate fully and truthfully with the SFO, and to review and maintain its existing internal controls, policies and procedures regarding compliance with the Bribery Act 2010. In its press release, the SFO highlighted the fact that the company appointed a new Executive Chairman in 2014, who identified the wrongdoing and ordered an internal investigation, which led to the company reporting matters to the SFO and the U.S. Department of Justice in 2015.

Finally, as outlined above, in January 2020, the DPA against Airbus SE was approved. This record-breaking settlement is considered later in the *In-Depth* section of this publication.

SIGNIFICANT INVESTIGATION DEVELOPMENTS

In March 2019, the SFO announced that it had opened criminal investigations against a number of individuals associated with London Capital & Finance plc. The Financial Conduct Authority (FCA) and others are providing assistance to the SFO.

In May 2019, the SFO opened a joint investigation with its Dutch counterpart in relation to biodiesel trading at Greenergy (a U.K.-based distributor of petrol and diesel for motor vehicles) and certain connected third parties. In opening its investigation, the SFO conducted searches at five sites across the U.K. and additional sites in the Netherlands and Belgium. To date, four individuals have been arrested and released without charge. The investigation continues.

In July 2019, the SFO confirmed that it had opened an investigation into the activities of the De La Rue Group and its associated persons in relation to suspected corruption in South Sudan.

The SFO's long-running investigation against ENRC and its acquisition of mineral assets in Africa continues to grab the headlines. Although the investigation began in 2013, no charges have been brought against the company, its employees or agents to date. In November 2019, the SFO confirmed that ENRC had failed in its attempt to seek a judicial review designed to force the body to reinstate an independent examination of the case. In November 2018, the SFO had appointed retired High Court judge, Sir David Calvert-Smith, to carry out an independent review following demands made by ENRC. However, the review was suspended in March 2019 when ENRC filed a separate civil claim seeking more than $90 million from the SFO for alleged wrongful conduct by inducing the company's former lawyers to act in breach of contract.

In December 2019, following an announcement by Glencore plc, the commodity trading and mining company, the SFO confirmed that it is investigating suspected bribery in the conduct of business by the Glencore group of companies, its officials, employees, agents and associated persons.

OTHER MATTERS OF INTEREST

In December 2019, the High Court refused an application by Tesco plc to withdraw an admission made in its defense as part of the ongoing civil proceedings brought by investors who argue that they have suffered a loss resulting from false and misleading trading statements issued by the company. In refusing the application, Mr. Justice Supperstone relied, at least in part, on the fact that when entering into the DPA with the SFO and agreeing the terms of the Final Notice with the FCA, Tesco entities made similar admissions. The case serves as a timely reminder that reaching a settlement in one set of proceedings may well have consequences in others.

Interestingly, Lisa Osofsky used the announcement of the DPA against Airbus SE to call for an overhaul of the U.K.'s legal regime to make it easier to prosecute corporate entities. As many readers will be aware, this is not the first time that Ms. Osofsky has raised the issue. In 2018, she called for an extension of corporate criminal liability and the creation of an all-encompassing failure to prevent fraud offense, akin to the offenses under the Bribery Act 2010 and the Criminal Finances Act 2017.

Back in 2014, the then-Attorney General, Jeremy Wright, mooted the creation of a failure to prevent serious economic crime offense. However, nothing came of his proposals.

As matters currently stand, there appears to be little appetite to reform the laws concerning corporate criminal liability generally, although there remains the possibility that further "failure to prevent" offenses will be introduced in an effort to combat particular types of criminal activity. It will be interesting to see whether Ms. Osofsky's ideas gain any greater traction this time on the back of the SFO's record-breaking outcome against Airbus SE.

LOOKING AHEAD

Like most other law enforcement and prosecution agencies, the SFO remains under pressure to deliver timely outcomes in relation to some of the U.K.'s most high-profile investigations. There can be little doubt that Ms. Osofsky's highlighting of the benefits to individuals and organizations of cooperating with the SFO is designed to encourage others to come forward and engage with the agency. In turn, this should lead to a reduction in the time it takes to investigate matters and resolve any proceedings that may follow.

In the short term, the SFO is bound to enjoy a "bounce" following the settlement reached with Airbus SE, but in the weeks and months to come, a number of other high-profile cases are due to reach a conclusion. In our next edition of *U.K. Business Crime Review*, we will be examining whether Ms. Osofsky's determination to use a broader range of tools to deliver results has borne fruit.

FINANCIAL CONDUCT AUTHORITY

On the business crime front, the trends seen at the Financial Conduct Authority (FCA) in recent years continued in 2019—an ever-increasing number of investigations afoot; an increased willingness to pursue individuals and firms on a criminal basis; and a keen focus on firms' maintenance of systems and controls to prevent and detect financial crime.

However, the sheer scale of the endeavors it has embarked upon and the time it is taking to deliver outcomes has led many to question whether the FCA's Enforcement and Market Oversight Division (EMO) has bitten off more than it can chew.

ENFORCEMENT ANNUAL PERFORMANCE REPORT

On 9 July 2019, EMO published its *Annual Performance Report* (the Annual Report), which provides an overview of EMO's activities from 1 April 2018 to 31 March 2019.

In the 12 months following 1 April 2018, 343 investigations were opened and 189 were closed, leaving a total of 650 ongoing as at 31 March 2019. That figure equates to more investigations than investigators employed by the Division. When considering this number, it is also important to note that, as the Annual Report stresses, one investigation may relate to multiple firms and/or individuals and comprise multiple allegations of misconduct.

The latest figure, a 29% increase on the previous year, continues the recent pattern of an ever-increasing number of investigations being conducted by EMO. As at 31 March 2016, there were just 237 ongoing investigations, but this figure rose to 414 in 2017 and 504 in 2018.

Of the 650 investigations, 136 were categorized as relating to "unauthorised business," 101 to "retail conduct," 96 to "insider dealing," 88 to "financial crime" and 70 to "culture/governance." These categories were the "top five" in a list of 15. The number of investigations being carried out increased in all but three of the 15 categories listed.

Beyond the broad categories, the Annual Report does not detail the types of conduct or criminal offenses that gave rise to an investigation. Similarly, the Annual Report does not provide a breakdown of the number of investigations being carried out on a regulatory basis, a criminal basis or a "dual track" basis (i.e. those that may lead to a regulatory and/or criminal outcome).

The total number of outcomes published in 2019 amounted to 288—29 fewer than the previous year. Of those 288 outcomes, the vast majority (238) concerned the variation, cancellation or refusal of authorization, approval or permissions. Of the remaining 50, 12 were described as "criminal," 16 the imposition of a financial penalty, 20 a prohibition and two redress or restitution. At this point, it is equally important to remember that one investigation can result in multiple outcomes.

APPROACH TO ENFORCEMENT

The publication of the Annual Report followed hot on the heels of the launch of the *FCA Mission: Approach to Enforcement* in April 2019, which is the latest in a series of mission statements designed to provide transparency to the FCA's activities and to explain its approach in greater depth.

In launching the policy statement, the FCA described the overriding principle as "substantive justice"—ensuring that investigations are carried out in a consistent and open-minded way to get to "the right outcomes." The key takeaways from the document are set out below.

Opening an investigation does not mean we believe misconduct has occurred or that anyone involved in the investigation is guilty of misconduct. The purpose of the investigation is to get a full understanding of the facts so that we can make a decision about whether and, if so, what kind of action may be necessary.

If it appears that individuals may be involved in the suspected serious misconduct of a firm, we will investigate those individuals at the same time we investigate the firm. This allows relevant facts and matters to be considered together, in the round. This is especially important where relevant individuals have had a senior management or governance role in the circumstances under investigation.

We recognize that we must act fairly, and make sure that people suspected of wrongdoing are not under investigation for any longer than is necessary. Where it is clear there is no substance to suspicions or evidence of serious misconduct it is important that we end investigations promptly. In these cases, we may use other powers to address our concerns...

We take a strategic approach in our investigations. We aim to quickly identify the heart of the case so we can focus on the key evidence and decide whether to continue with or close the investigation. We also keep

the scope of our investigation under review, whether that is extending its scope or narrowing it and certain aspects of the investigation.

We do not pre-judge the outcome of an investigation. If we investigate a breach that might be the subject of criminal or civil proceedings, we will not decide straight away whether we are investigating to determine a criminal or civil breach. For example, in money-laundering and market abuse cases, an investigation might lead to either regulatory or criminal proceedings. Our approach is to make sure we fully understand what may have happened and make a decision based on the best available evidence.

Few can argue with the principles set out above. It is in the interests of all concerned for EMO to conduct expeditious, fair and open-minded investigations, but many commentators have noted that the practical realities appear to be very different, with many firms and individuals facing extended periods under investigation with little or no progress being made towards resolution.

On any view, continuing to increase the number of investigations at the current rate is simply unsustainable without a significant increase in resources. As matters currently stand, those resources do not appear to be forthcoming, so it will be interesting to see how EMO tackles its substantially greater workload in the coming months.

MONEY LAUNDERING REGULATIONS 2017

One area of EMO's focus that continues to attract a significant amount of attention is its enforcement of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, commonly referred to as the MLRs, against FCA-regulated firms and individuals.

Many readers will be very familiar with the MLRs. They came into force on 26 June 2017, replacing the Money Laundering Regulations 2007, and gave effect to the EU's Fourth Money Laundering Directive.

The MLRs apply to those carrying on business (in designated sectors) in the U.K.—a broad definition that includes any business whose registered or head office is in the U.K. if the day-to-day management of the business is the responsibility of that office or another establishment maintained in the U.K. They set out a range of regulatory standards concerning AML policies, training, due diligence etc.

A breach of the MLRs can be punished with a range of civil and criminal sanctions. If prosecuted, firms may be subjected to unlimited fines and individuals may be imprisoned for up to two years.

Responsibility for enforcing compliance with the MLRs rests with the designated supervisory authority depending upon the sector in which the business or individual operates. The FCA is the designated supervisory authority under the MLRs for those firms that fall within its remit under the Financial Services and Markets Act 2000 (FSMA).

Firms have been pursued for breaches of their AML and counter-terrorist financing systems and controls under the FCA's broader regulatory framework for several years. In our view, there is very little to separate a regulatory investigation under the MLRs from a regulatory investigation under that wider framework. However, it is the fact that EMO is showing an increased willingness to pursue criminal investigations under the MLRs against firms and individuals that has caused a stir over the past couple of years.

During a speech in April 2019 at Global Investigations Review Live, Mark Steward, EMO's Executive Director, sought to explain the FCA's change in approach.

It would be inconsistent with the investigative mindset to narrow the scope of potential outcomes provided for by the law before you have made any inquiries or been able to assess the nature of the matter under investigation.

Moreover, this practice brings AML investigations into line with the FCA's practice in market abuse investigations, which have been conducted on a "dual track" basis for many years as well.

More importantly, I think it is time that we gave effect to the full intention of the Money Laundering Regulations, which provide for criminal prosecutions. In making poor AML systems and controls potentially a criminal offense, the MLRs are signaling that, in egregious circumstances, MLR failures let down the whole community.

This does not mean every investigation where we think there is a case to answer will or should be prosecuted in this way. I suspect criminal prosecutions, as opposed to civil or regulatory action, will be exceptional. However, we need to enliven the jurisdiction if we want to ensure it is not a white elephant and that is what we intend to do where we find strong evidence of egregiously poor systems and controls and what looks like actual money-laundering.

The change in approach is in line with the broader principles outlined in the FCA's Approach to

Enforcement. However, it also follows criticism from the Financial Action Task Force in 2018 at the lack of prosecutions brought under the MLRs and the 2007 Regulations.

In March 2019, *The Times* reported that no prosecutions had been brought under the MLRs and only 11 had been brought under the 2007 Regulations. None of those prosecutions were brought by the FCA.

Even though Mr. Steward stated in April 2019 that a "large number" of investigations were entering "important phases", the FCA confirmed in January 2020 that it is yet to prosecute any firm or individual under the MLRs in response to a request made under the Freedom of Information Act 2000.

Readers may also wish to note that although the powers available to the FCA under the MLRs and FSMA are dependent on the conduct or offense that is being investigated, once in receipt of material, the FCA is entitled to use it to prosecute any criminal offense, providing such actions accord with its statutory objectives and are not contrary to an express statutory prohibition. The FCA frequently prosecutes criminal offenses for which it is not afforded investigation powers, such as fraud, perverting the course of justice and forgery. Therefore, in principle, nothing prevents the FCA from prosecuting substantive money laundering offenses under the Proceeds of Crime Act 2002, some of which carry maximum sentences of imprisonment of 14 years, following an investigation under the MLRs.

SIGNIFICANT CRIMINAL OUTCOMES

Despite the significant increase in the number of investigations carried out by EMO in recent years, only one criminal trial was prosecuted to a conclusion in 2019. It concerned Fabiana Abdel-Malik and Walid Choucair, who were each convicted of five offenses of insider dealing and sentenced to three years' imprisonment in June 2019.

At the time of her offending, Ms. Abdel-Malek was a senior compliance officer employed by UBS in its London office. She used her position to identify inside information, which she passed to Mr. Choucair, an experienced day trader and family friend. Armed with the information, he proceeded to deal in Contracts for Difference (CFDs) through an account held in the name of a company incorporated in the British Virgin Islands with a trading address in Switzerland. In each of the five instances, he opened positions in relation to companies that were the subject of actual or potential takeovers ahead of press articles or company announcements that caused their share price to increase substantially. As a result, Mr. Choucair made profits in the region of £1.4 million.

In July 2019, following the lifting of reporting restrictions, the FCA was able to announce that Richard Baldwin had been convicted of money laundering, in his absence, following a trial at Southwark Crown Court in 2017. On 3 September 2019, he was sentenced to a total of five years and eight months' imprisonment for the offense and for breaching the terms of a restraint order imposed in June 2011 under the Proceeds of Crime Act 2002, which prevented him from dealing with, disposing of or diminishing the value of any asset in which he had an interest.

Mr. Baldwin's conviction followed those of Martyn Dodgson and Andrew Hind in May 2016 for conspiracy to insider deal between November 2006 and March 2010. All three convictions were secured following one of the FCA's largest and longest-running investigations, known as Operation Tabernula.

Mr. Baldwin was a business partner of Mr. Hind—the two men ran a luxury watch business from offices in London. In order to avoid receiving the profits from the traders who traded on their behalf, Mr. Baldwin set up a company in Panama with a bank account in Zurich, which was used to receive £1.5 million. The sum represented the profits from trading in just one stock—Scottish & Newcastle plc. The vast majority of the sum was then dissipated through other Panamanian companies and offshore accounts. Following the search of Mr. Baldwin and Mr. Hinds' business premises in March 2010, Mr. Baldwin closed the accounts of the Panamanian companies the funds had passed through.

In June 2011, Mr. Baldwin was notified of the restraint order. Within a fortnight, he had flown twice to Switzerland and withdrawn the equivalent of £114,000 in cash, and liquidated assets worth more than £82,500. Over the next six months, he accessed safety deposit boxes in Switzerland and the U.K., and dealt with the assets contained therein, including a number of high value watches. In the two-year period thereafter, Mr. Baldwin disposed of other assets, which he had failed to repatriate to the U.K., and dealt with undisclosed income. He admitted breaching the terms of his restraint order in November 2015, but his punishment was adjourned to await the outcome of his criminal trial.

In 2017, shortly before the money laundering trial was due to commence, Mr. Baldwin, who was on bail at the time, absconded. He was tried in his absence and convicted. An arrest warrant has been issued, but he remains at large.

While 2019 saw only one criminal trial prosecuted by the FCA, in December 2019, a confiscation order in the sum of £5,118,018 was made against Dharam Prakash Gopee under the Proceeds of Crime 2002. The order, which is the largest ever secured by the FCA, must be paid within three months or Mr. Gopee will face 11 years in prison, in addition to the sentences he has already received for his wrongdoing. He has also been banned from leaving the U.K. until the order is paid.

The confiscation proceedings followed his conviction for illegal money lending in February 2018, for which he was sentenced to a total of three and a half-years' imprisonment, having already been committed to prison on two separate occasions for breaching the terms of a restraint order.

In 2019, the FCA also secured confiscation orders against:

- Muhammad Mirza (£1,190,128), Samrat Bhandari (£376,606), Michael Moore (£154,984) and Paul Moore (£29,736.45) following their convictions in 2017 for operating an illegal investment scheme;
- Mark Starling (£291,070) following his conviction in 2018 for defrauding investors out of almost £3 million by purporting to operate an investment fund; and
- Manraj Singh Virdee (£171,913) following his conviction in 2018 for defrauding investors by promoting an unauthorized deposit taking scheme marketed as an "investment package."

In each of the cases outlined above, sums recovered will be used to compensate the victims of their crimes.

The only criminal proceedings publicly announced by the FCA in 2019 were against Konstantin Vishnyak, a former employee of VTB Capital, who is alleged to have breached section 177(3)(a) of FSMA by deleting the WhatsApp application from his mobile telephone whilst subject to an investigation for suspected insider dealing. Mr. Vishnyak's case was transferred to Southwark Crown Court in September 2019. He awaits trial.

These proceedings mark the first time that the FCA has prosecuted the offense, which prevents a person who knows or suspects that an investigation is being conducted from falsifying, concealing, destroying or otherwise disposing of material relevant to such an investigation, although the agency has successfully prosecuted other individuals for perverting the course of justice by concealing or destroying evidence. The section 177 offense carries a maximum sentence of two years' imprisonment and/or an unlimited fine.

SIGNIFICANT REGULATORY OUTCOMES

In 2019, the FCA imposed 21 financial penalties totaling £392,303,087. Fifteen of the penalties, totaling £312,730,600, were imposed against firms.

Whilst regulatory proceedings are not the focus of this publication, a number of outcomes from 2019 demonstrate that the FCA remains focused on the adequacy and effectiveness of the systems and controls employed by firms to prevent and detect financial crime.

The largest penalty of £102,163,200 was imposed against Standard Chartered Bank in April 2019 for breaches of the MLRs. The FCA found "serious and sustained" shortcomings in AML controls relating to customer due diligence and ongoing monitoring between 2010 and 2013. The FCA also found that the Bank failed to ensure that its UAE branches applied U.K. equivalent AML and counter-terrorist financing controls between 2009 and 2014, highlighting the far-reaching effects of the MLRs. In support of its findings, the FCA highlighted the following examples:

- opening an account with three million UAE Dirham (approximately £500,000) in cash in a suitcase with little evidence that the origin of the funds had been investigated;
- failing to collect sufficient information on a customer exporting a commercial product which could, potentially, have a military application. The product was exported to over 75 countries, including two jurisdictions where armed conflict was taking place or was likely to be taking place; and
- not reviewing due diligence on a customer despite repeated "red flags," such as a blocked transaction from another bank indicating a link to a sanctioned entity.

In this case, the Bank agreed the findings of fact and liability, but argued that the penalty originally determined by the FCA was too high. The Regulatory Decisions Committee agreed and reduced the penalty from £155 million to £102 million.

Interestingly, despite the publicity surrounding the increased number of "dual track" investigations concerning breaches of the MLRs, the FCA chose to pursue a regulatory outcome in response to the Bank's conduct. This may indicate that, as far as firms as opposed to individuals are concerned, breaches of the MLRs are more likely to be marked by regulatory rather than criminal sanctions.

Also in April 2019, the Upper Tribunal upheld the FCA's decision to impose a financial penalty of £409,300 against Linear Investments Ltd for failing to take reasonable care to organize and control its affairs responsibly and effectively with adequate risk management systems in relation to the detection and reporting of potential instances of market abuse.

The FCA found that in the period from 14 January 2013 to 9 August 2015, the volume of trades routed through the firm to its brokers was at a level that meant that it was not capable of being monitored by the manual only process that was in place. The firm's reliance on post-trade surveillance by underlying brokers to discharge its regulatory obligation was incorrect and, at all times, the firm remained responsible for ensuring that it had effective post-trade surveillance systems in place.

The decision of the Upper Tribunal was the first under a newly introduced process that allows firms or individuals under investigation to enter into a contract called a "focused resolution agreement," under which certain elements of the case can be agreed. In this instance, Linear Investments Ltd agreed the matters of fact and liability, but disputed the penalty to be imposed. The Upper Tribunal rejected the submissions made on behalf of the firm and upheld the penalty imposed by the FCA. It is worth noting that a firm or individual who agrees to all of the underlying facts and the nature of the misconduct can still enjoy a 30% reduction in the penalty to be imposed even if they challenge it, as happened in this case.

In March 2019, UBS was fined £27,599,400 for failing to ensure that it provided complete and accurate information in relation to approximately 86.67 million reportable transactions. UBS also erroneously reported 49.1 million transactions to the FCA that were not, in fact, reportable. In reaching its decision, the FCA highlighted that effective market oversight relies on the complete, accurate and timely reporting of transactions to aid the supervision of firms and markets, and to help identify instances of market abuse and financial crime.

In June 2019, Bank of Scotland was fined £45,500,000 for failing to disclose information to the FCA and law enforcement agencies about its suspicions that fraud may have occurred within its Reading-based Impaired Assets Team over a period of more than two years, from 2007 to 2009. The FCA also banned four individuals from working in the financial services industry due to their roles in the fraud.

OTHER MATTERS OF INTEREST

From 9 December 2019, the Senior Managers & Certification Regime, commonly referred to as SMCR, has applied to all FCA-regulated firms. The Regime, which has applied to all banks, building societies, credit unions and investment firms designated by the Prudential Regulation Authority since 2016, has been hailed as another milestone in establishing healthy cultures and effective governance within financial services firms. It was introduced following a number of high-profile scandals in order to create a system of personal accountability through which firms and their staff would have a clear understanding of who was responsible for what (i.e. those within senior management with an FCA-prescribed senior management function).

The FCA has not released details of how many of its investigations concern "senior managers." However, anecdotal evidence suggests that the number of investigations is limited and there have been very few publicly-announced investigations or outcomes since SMCR's introduction. That said, the number is now expected to increase following the extension of SMCR to all other regulated firms, which tend to be smaller. This makes attributing acts and omissions to senior managers far more straightforward.

On 10 January 2020, the U.K.'s revisions to the MLRs required under the EU's Fifth Money Laundering Directive (5MLD) came into force following the Government's introduction of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019. Among other things, the revisions appoint the FCA as the supervisor of U.K. crypto-asset businesses for AML and counter-terrorist financing purposes. The implementation of 5MLD is discussed further in the *In-Depth* section below.

The FCA has faced significant criticism over its regulation of London Capital & Finance plc (LC&F), which entered administration on 30 January 2019. LC&F had been given permission by the FCA only for "advising" and "arranging" activities, but raised over £200 million from mostly U.K. retail investors. Its administration followed FCA action in December 2018 that required the firm to withdraw promotional material relating to its marketing of retail investment products, many of which were labelled at the time as eligible for investment savings account (ISA) status. The FCA, in taking this decision, concluded the promotional materials to be misleading, unfair and unclear. Alongside the FCA's actions, Her Majesty's Revenue & Customs (HMRC) also revoked LC&F's approval as an ISA account manager. In December 2019, the FCA took broader action, prohibiting any regulated firm from issuing or selling non-transferable bonds (which are sometimes, especially when issued by corporates, referred to as "mini-bonds").

There are widespread concerns that this FCA-authorized firm, and formerly HMRC-approved ISA account manager, was used to operate an alleged "Ponzi scheme." The administrators are currently predicting a return to investors of as little as 25% of their investment. In March 2019, the Serious Fraud (SFO) announced that it had arrested and opened criminal investigations against a number of individuals associated with LC&F or its service provider, Surge Financial Limited. The FCA and others are providing assistance to the SFO.

An independent investigation led by former Court of Appeal judge, Dame Elizabeth Gloster is underway at the request of the FCA's Board and HM Treasury. The investigation will consider the FCA's actions, policies and approach to regulating LC&F.

LOOKING AHEAD

2020 is set to be a pivotal year for the FCA, and for EMO in particular, as it comes under increasing pressure to resolve a sizeable proportion of the investigations that have been underway for some time, and particularly those that relate to key priorities. It remains to be seen whether the much-anticipated developments promised by Mr. Steward, particularly in relation to prosecutions under the MLRs, will materialize.

Following Andrew Bailey's appointment as Governor of the Bank of England—a position he will take up on 16 March 2020 – the FCA will also be searching for a new CEO. In the short term, the post is to be filled by Chris Woolard, the FCA's Director of Strategy and Competition, while the search for Mr. Bailey's successor gets underway. It will be interesting to see whether the appointment of a new CEO will signal a change in direction in EMO's priorities.

NATIONAL CRIME AGENCY

Like many of the U.K.'s other law enforcement agencies, the National Crime Agency (NCA) has a broad portfolio. However, it's primary objective is to protect the public from those who pose the greatest threat to the United Kingdom by cutting serious and organized crime, which it estimates costs the U.K. economy at least £37 billion a year. Many commentators believe the figure is likely to be significantly greater than that.

Its work aims to tackle some of the most serious offending, usually with a national or international dimension, such as terrorism, human trafficking, drug smuggling, sexual exploitation and cybercrime, by using a variety of tools and measures, including the commencement of prosecutions and civil proceedings, as well as intelligence gathering and disruption techniques. However, in this section, we will focus on its recent work to tackle serious economic crime.

NATIONAL ECONOMIC CRIME CENTRE

In December 2017, the Home Secretary announced the creation of the National Economic Crime Centre (NECC) to "task and coordinate the national response to economic crime, backed by greater intelligence and analytical capabilities." Although housed within the NCA, the U.K. Government's hope was that it would draw on "expertise from across government, law enforcement and criminal justice agencies, as well as new resources provided by the private sector."

In October 2018, the NECC was officially launched and in February 2019, Graeme Biggar was appointed as its first Director General, reporting to the Director General of the NCA, Lynne Owens. Prior to his appointment, Mr. Biggar had been the Director of National Security at the Home Office since 2016 and before that, the Chief of Staff to the Secretary of State for Defence from 2013.

The creation of the NECC has brought together staff from the NCA, the Serious Fraud Office (SFO), the Financial Conduct Authority (FCA), Her Majesty's Revenue & Customs (HMRC), the City of London Police, the Crown Prosecution Service and the Home Office, as well as the private sector, to identify and prioritize the most appropriate type of investigation, whether criminal, civil or regulatory, in order to ensure "maximum impact." The Government views the establishment of the NECC as a central plank in its Economic Crime Plan for 2019 to 2022, which was published in July 2019.

The creation of the NECC has been widely welcomed as a way of tackling what has often been described as a "fragmented approach" to tackling serious economic crime in the U.K. The Government no doubt hopes that its establishment will go a long way to deliver a joined-up strategy from a variety of law enforcement agencies and prosecuting bodies whose work is frequently divided up based on the sums involved, the crime type, the sector concerned or geographical location.

It is too soon to say whether the NECC is meeting its objectives, but it is almost certainly under tremendous pressure to do so. In future editions of *U.K. Business Crime Review*, we will be examining its work in a little more detail.

JOINT MONEY LAUNDERING INTELLIGENCE TASKFORCE

The NECC includes the Joint Money Laundering Intelligence Taskforce (JMLIT), which was created in 2015 as "a partnership between law enforcement and the financial sector to exchange and analyse information relating to money laundering and wider economic threats." In order to carry out its work, JMLIT relies on existing information sharing gateways, such as section 7 of the Crime and Courts Act 2013, which allows any person to disclose information to the NCA if the disclosure is made for the purposes of the exercise of an NCA function.

JMLIT includes representatives from over 40 financial institutions, as well as the NCA, the SFO, the FCA, HMRC, the City of London Police, the Metropolitan Police Service and Cifas—the fraud prevention membership association. Since its inception, it has supported or developed over 500 law enforcement investigations, which have directly contributed to over 130 arrests and the seizure or restraint of more than £13 million worth of assets. In addition, JMLIT's private sector members have identified over 5,000 suspect accounts linked to money laundering activity and commenced more than 3,500 internal investigations. In its Mutual Evaluation published in December 2018, FATF highlighted JMLIT as "a particularly strong feature" of the U.K.'s AML regime and its successes are widely viewed as having led to the creation of the NECC.

Establishing effective public-private partnerships is a key theme in the Government's Economic Crime Plan. One of its fundamental aims is "for the public and private sectors to jointly deliver a holistic plan that defends the U.K. against economic crime, prevents harm to society and individuals, protects the integrity of the U.K. economy, and supports legitimate growth and prosperity." Both HM Treasury and the Home Office

believe that "by harnessing the capabilities, expertise and information of both the public and private sectors, we can be a world-leader in the global fight against economic crime."

Of course, the private sector, and the financial services sector in particular, already play a significant role in the U.K.'s fight against economic crime. However, few would argue that there is scope to develop a more effective and wide-reaching partnership. What remains to be seen is how the Government envisages such a partnership operating in practice. Will there be greater scope for information sharing between financial institutions and increased feedback from law enforcement agencies when information is provided? Will the Government embark on a more collaborative approach to legislative reform and the development of financial crime policy? Will there be more opportunities to develop and share best practices, to pool resources or to cooperate in the building of improved IT systems and advanced technological solutions?

We have little doubt that many financial institutions operating in the U.K. are likely to welcome the opportunity to develop a genuine, public-private partnership. The concern is that the U.K. Government may view such a measure simply as a way of shifting the burden of fighting economic crime to the private sector with ever-increasing regulatory burdens and demands for funding.

FINANCIAL INTELLIGENCE UNIT

The U.K.'s Financial Intelligence Unit (FIU) sits within the NCA and is responsible for receiving, analyzing and disseminating financial intelligence gathered from Suspicious Activity Reports (SARs), which individuals and firms, and particularly those operating in regulated sectors, are required to submit if they suspect money laundering or terrorist financing. The FIU also maintains a secure network with FIUs throughout the world to receive and share information in order to fight money laundering and terrorist financing.

In its Annual Report, the FIU revealed that it received a record 478,437 SARs between April 2018 and March 2019—a 3.13% increase on the previous year when 463,938 were submitted. This equates to 1,310 a day.

Of those filed, 34,543 were Defence Against Money Laundering (DAML) SARs—a 52.72% increase on the previous year. As many readers will be aware, DAML SARs allow individuals or firms to seek consent from the FIU to deal with property that they suspect is in some way criminal. Of those submitted, 34,151 related to money laundering and 392 related to terrorist financing.

As a result of DAML SARs being filed, the FIU calculated that £131,667,477 was denied to criminals—a staggering 153.66% increase on the previous year's figure of £51,907,067. The significant increase is largely thought to be due to the introduction of Account Freezing Orders (AFOs), which allow a number of law enforcement and prosecuting agencies to apply to a court to freeze the balance of a bank account if it has reasonable grounds for suspecting that the money held is property obtained through, or to be used in, unlawful conduct. Thereafter, the monies held may be forfeited if a person with an interest in the account fails to respond to an Account Forfeiture Notice issued by the relevant agency within the permitted period or if a court is satisfied, on the balance of probabilities, that the balance is property obtained through, or to be used in, unlawful conduct. The new powers, which came into force on 17 April 2018, were introduced to Part V of the Proceeds of Crime Act 2002 by the Criminal Finances Act 2017.

As an example of the impactful way in which the new powers may be used, in December 2019, the NCA announced that it had agreed to a settlement in the region of £190 million with a family that owned large property developments in Pakistan and elsewhere. The announcement followed an investigation into Malik Riaz Hussain, a Pakistani national, whose business is one of the largest, private-sector employers in his home country. As part of that investigation, the NCA obtained AFOs over a total of nine bank accounts containing around £140 million. The balance of the settlement takes account of a London property with an estimated value of £50 million. All sums forfeited will be returned to the State of Pakistan.

The U.K.'s FIU has come in for a fair amount of criticism in recent years, not least from the Financial Action Task Force (FATF) during its recent Mutual Evaluation, who observed that the legal framework under which it operates needed "significant improvements." In addition, FATF identified a need "to enhance the resources and capabilities" available to the FIU—a recommendation it had also made in its previous assessment.

In fairness to the U.K. Government, by the time FATF delivered its assessment in December 2018, it had already tried to tackle some of the perceived weaknesses in the operation of the FIU by committing further resources. However, many of the issues that need to be addressed are challenging and complex, such as the technological infrastructure and legal framework that underpin the SARs regime.

REFORM OF THE SARS REGIME

Since as long ago as April 2016, the Home Office promised "fundamental reform" of the SARs regime. In December 2017, it invited the Law Commission to review limited aspects of the U.K. anti-money laundering and counter-terrorism financing regime, including reviewing the legislative framework underpinning the SARs regime.

In June 2019, the Law Commission published its recommendations in relation to the SARs regime, which included:

- creating an advisory board with oversight for the regime, with a remit to oversee the drafting of guidance, to measure the effectiveness of the regime and advise the Secretary of State on ways to improve it;
- retaining the consent regime, subject to amendments to improve effectiveness;
- statutory guidance on key legislative concepts (e.g., suspicion);
- prescribing the form in which suspicious activity is reported and making use of technology to devise an online interactive form;
- an exemption to allow ring-fencing of suspected criminal property by a credit or financial institution;
- maintaining the status quo for the reporting of "all crimes;"
- extending the circumstances in which a reporter may have a reasonable excuse not to make a voluntary disclosure; and
- further research into the utility of thematic reporting or geographical targeting orders, which remove the reporter's discretion to assess suspicion.

On any view, the recommendations put forward were relatively modest. However, the U.K. Government is yet to commit to implementing them while it undertakes a wider assessment of the U.K.'s AML regime.

The Government has a range of options. In the short term, it could implement so-called "quick wins"—those that do not require legislative change or significant investment—such as changes to the technological infrastructure and reporting mechanisms. In the longer term, the U.K. could also decide to implement a transaction reporting regime, which would require reporters to file reports when certain objective criteria are met (e.g., value or type of transaction). Such regimes exist in a number of other jurisdictions, including the U.S. and Australia.

On the legislative front, the Government may seek to tweak the regime in line with the Law Commission's recommendations or go further. A complete overhaul of the Proceeds of Crime Act 2002 is by no means "off the table," but such a measure is likely to take several years to implement. It may also decide to tackle particular issues under the current regime, such as how to deal with activities that would be illegal in the U.K., but are legal in the jurisdiction in which they take place, such as cannabis cultivation for specified purposes.

Whatever decisions the Government decides to take, there are two fundamental issues that it will almost certainly want to address. First, how to improve the quality of the information provided in the ever-increasing number of SARs filed, and second, how to improve the way in which such information can be used to develop investigations and law enforcement strategies more generally.

UNEXPLAINED WEALTH ORDERS

As part of the amendments to the Proceeds of Crime 2002 introduced by the Criminal Finances Act 2017, a number of law enforcement and prosecuting agencies, including the NCA, the SFO, the FCA and HMRC, gained a new investigative tool to use as part of a civil recovery investigation—the Unexplained Wealth Order (UWO). The relevant statutory provisions came into force on 31 January 2018.

Under Part V of the Proceeds of Crime Act 2002, the High Court is empowered to make a civil recovery order against property that it determines, on the balance of probabilities, to be "recoverable property" (i.e. property obtained through, or to be used in unlawful conduct). Any party identified as having an interest in the property will be a party to the claim, although the claim is *in rem* (i.e. against the property).

A UWO is an order made by the High Court that compels a person holding property worth more than £50,000 to provide information as to how they came to obtain the property where there are reasonable grounds to suspect that their lawfully obtained income would have been insufficient to allow them to obtain the property in question. If the person fails, without reasonable excuse, to comply with the terms of a UWO within the permitted timeframe, the property is presumed to be "recoverable property" for the purposes of any civil recovery proceedings.

A UWO can be made against a Politically Exposed Person (PEP) from outside the European Economic Area (EEA), or a person reasonably suspected of involvement in serious crime (anywhere in the world), or someone connected to either category of person. Like in civil recovery proceedings, the High Court is able to make a

freezing order over any property that is the subject of a UWO.

USE OF UWOS

In February 2018, the NCA secured the first-ever UWOs in relation to two high-value properties in the South East of England worth a total of £22 million. At the time, the identity of the holder of the properties was not publicized. However, in May 2019, the High Court agreed to release documents to the press that revealed the holder to be Zamira Hajiyeva, the wife of the convicted former Chairman of the International Bank of Azerbaijan, who is currently serving a 15 year sentence for fraud and embezzlement.

Much to the interest of the press, the court documents released included details of the spending habits of Mrs. Hajiyeva, which revealed a total expenditure of £16 million at Harrods in London. The documents also revealed that the NCA had seized a diamond ring worth in excess of £1 million and other items of jewelry totaling around £400,000, suspecting them to have been acquired with the proceeds of crime.

In July 2018, Mrs. Hajiyeva had brought a challenge to the imposition of the UWO. Among various grounds, she argued that she was not a PEP as this was reliant on her husband being a PEP, which, in turn, was reliant on her husband working for a state-owned enterprise. She also challenged whether there were reasonable grounds to suspect that her known sources of lawfully obtained wealth were insufficient to allow her to obtain the property.

The challenge was dismissed by the High Court in October 2018. On these two specific grounds, the Court held (i) that the evidence of the relevant government having a majority shareholding in the bank meant that it constituted a state-owned enterprise and (ii) that the evidence that her husband was a state employee between 1993 and 2015 meant it was very unlikely that his lawful income would have been sufficient to purchase the properties for £11.5 million.

Mrs. Hajiyeva appealed against the High Court's decision. The Court of Appeal heard the appeal in December 2019 and delivered its judgment on 5 February 2020. The Court upheld the High Court's decision and confirmed that Mrs. Hajiyeva was a PEP as a result of her husband's former employment. In that regard, the Court stated that a broad approach should be taken when assessing whether an entity is a "state-owned enterprise." The Court also confirmed that neither the privilege against self-incrimination nor spousal privilege applied to the UWO regime, and even if they did, the U.K. Parliament had clearly intended such privileges to be abrogated. Mrs. Hajiyeva must now comply with the UWO made against her and provide the NCA with a full account of the source of her wealth unless she is successful in persuading the U.K. Supreme Court to hear her case—the Court of Appeal has refused permission to appeal.

In May 2019, UWOs were obtained in relation to three residential properties in London believed to be linked to a PEP involved in serious crime. It is understood that the properties were originally bought for more than £80 million and held by offshore companies.

In July 2019, the NCA obtained its first UWO against an individual with suspected links to serious criminals. The businessman from the North of England was ordered to reveal the source of his £10 million property portfolio. This was followed in January 2020 with an AFO freezing £1.13 million and most recently, a Property Freezing Order in February 2020 preventing the sale of 17 addresses in Leeds, Cheshire and London. All of the orders relate to the same ongoing investigation.

Also in July 2019, a UWO was made against a Northern Irish woman with suspected links to paramilitary activity and cigarette smuggling. Under the terms of the UWO, she was required to explain how she financed the purchase of six properties worth around £3.2 million.

LOOKING AHEAD

It is almost certain that a number of issues will see the NCA and its work remain in the spotlight in 2020. First, many will be examining whether the creation of the NECC has delivered an improvement in the U.K.'s ability to tackle serious economic crime. Second, will be the U.K. Government's efforts to reform the SARs regime. In this respect, whether the role of the FIU should be enhanced is likely to be a topic for discussion. Third, all eyes will be on the NCA's use of the powers introduced under the Criminal Finances Act 2017 and whether its recent success in the Court of Appeal will embolden the agency in its use of UWOs. These are all issues that we are likely to return to in our next edition of *U.K. Business Crime Review*

HER MAJESTY'S REVENUE & CUSTOMS

As readers will be aware, Her Majesty's Revenue & Customs (HMRC) is the U.K.'s tax, payments and customs authority. The non-ministerial government department has a very broad remit and uses a wide range of tools, including civil and criminal sanctions, to ensure compliance with the U.K.'s tax, payments and customs regimes. However, in this section, we will concentrate on the recent steps HMRC has taken to tackle tax avoidance and evasion, and in particular, its sharpened focus on understanding how corporate entities are used, both knowingly and unwittingly, to facilitate serious economic crime.

TAX EVASION AND AVOIDANCE

In the Annual Report published in July 2019, Sir Jonathan Thompson, HMRC's CEO and Permanent Secretary at the time stated that the body used its powers to "respond to avoidance, evasion and attacks on the tax system." HMRC stated that during the reporting period—the 12 months from April 2018—it had collected £34.1 billion in additional taxes by tackling avoidance, evasion and non-compliance. HMRC also stated that at any one time, it is actively investigating around half of the U.K.'s largest businesses with a particular focus on 0.5% of businesses that appear, in its view, to demonstrate deliberate tax avoidance rather than a misunderstanding of the relevant statutory framework.

Recent figures have revealed that in the 12 months since April 2017, HMRC believes that its investigations against large businesses led to more than £9 billion in additional tax revenue being secured. HMRC also revealed that between 2014 and 2018, it was successful in 84% of tax cases brought against large businesses before the First Tier Tax Tribunal.

Since 30 September 2017, businesses can be held criminally liable if a person performing services for or on behalf of the business has facilitated a third party to evade tax. The Criminal Finances Act of 2017 creates criminal liability under two separate offenses. The offense set out under section 45 deals with U.K. tax evasion. The offense set out under section 46 deals with foreign tax evasion. Under both sections, it is a defense for a business to demonstrate that it had in place such prevention procedures as it was reasonable in all the circumstances to expect the business to have or that it was not reasonable in all the circumstances to expect the business to have any prevention procedures in place.

Despite the relevant laws being in force for more than two years, no-one has yet been prosecuted for either offense. However, in response to a recent request under the Freedom of Information Act 2000, HMRC stated that as of 31 December 2019, it was carrying out nine investigations in this area and that it had identified a further 21 potential investigations. It stated that the investigations and potential investigations concerned businesses in ten different sectors, including "financial services, oils, construction, labour provision and software development," ranging from "small businesses through to some of the U.K.'s largest organisations."

The numbers set out above are relatively low given HMRC's prediction back in 2018 that it would be bringing 100 prosecutions a year for offenses under the Criminal Finances Act 2017 by 2022. In future editions of *U.K. Business Crime Review*, we will be paying close attention to HMRC's progress in this area.

Of course in this space, it remains the case that criminal proceedings are more likely to be brought against individuals rather than corporate entities. In any given year, dozens of individuals will face investigation for tax evasion and a number of them will face prosecution. As is now tradition, in January 2020, HMRC released a list of its biggest criminal cases of 2019. Of the nine cases highlighted, several involved the fraudulent evasion of tax, serving to underline that tackling this issue remains a key priority for HMRC.

OFFSHORE TAX EVASION AND AVOIDANCE

In March 2019, HMRC published its revised "No Safe Havens" policy, which outlines how it intends to ensure offshore tax compliance. Since the release of the Panama Papers in 2016 and the Paradise Papers a year later, the use of entities in offshore jurisdictions to evade and avoid tax has remained a key focus. HMRC believes that the Panama Papers will lead to more than 400 criminal and civil investigations, and yield more than £190 million.

Since 2010, the U.K. Government has introduced over 110 measures to tackle offshore tax compliance. HMRC believes that those measures have secured over £200 billion and helped to reduce the "tax gap"—the difference between those sums that should be paid to HMRC and those that are paid.

In addition, HMRC highlights the U.K.'s role as a global champion of tax transparency and the fact that more than 100 jurisdictions have committed to exchange financial account information under the Common Reporting Standard—the mechanism developed by the Organisation for Economic Cooperation and Development in an effort to combat tax evasion.

As is the case with domestic tax evasion, criminal proceedings are more likely to be brought against individuals rather than corporate entities. In its most recent Annual Report, HMRC stated that between 2012 and 2019, it successfully prosecuted 34 individuals for offshore tax evasion and that a further 120 individuals are under criminal investigation for offshore tax offenses.

However, it should be noted that for all of the measures introduced to tackle domestic and offshore tax evasion and avoidance, HMRC's figures published in 2019 show that the overall U.K. "tax gap" increased to £35 billion over the twelve months to March 2018. That figure equates to 5.6% less than the amount HMRC believes ought to be paid.

ORGANIZED CRIME AND MONEY LAUNDERING

Between April 2018 and March 2019, HMRC believes it protected approximately £3 billion worth of assets that would have otherwise been exploited by organizations that carry out cross-border smuggling, exploitative labor fraud, transnational VAT fraud and various other crimes.

HMRC, in its role as a designated supervisor under the Money Laundering Regulations 2017, conducted 2,200 interventions and issued 131 penalties with a total value of £1.2 million between April 2018 and March 2019. HMRC also conducted 162 AML investigations and secured convictions for 32 money laundering-related offenses.

Money service bureaus remain a key target of HMRC's supervisory activities. In September 2019, a record £7.8 million fine was imposed against Touma Foreign Exchange Ltd. as a result of a number of "serious failures" under the Money Laundering Regulations 2017 relating to (i) risk assessments and associated record-keeping, (ii) policies, controls and procedures, (iii) fundamental customer due diligence and (iv) staff training.

Businesses should also be aware that HMRC has taken to carrying out focused activities against specific sectors in order to ensure AML compliance. For example, in February 2019, HMRC undertook a week of activity against estate agents during which officers visited more than 50 addresses to carry out "on the spot" checks.

LOOKING AHEAD

In 2020, all eyes will be on HMRC to see whether any of its investigations for failing to prevent the facilitation of tax evasion result in prosecutions and, if so, against whom. Recent trends indicate that this is bound to be an area that will attract further Parliamentary scrutiny too, which will mean that HMRC will face added pressure to deliver results.

As there appears to be no let-up in HMRC's interest in how corporate vehicles are used to facilitate serious economic crime, businesses should continue to ensure that their compliance frameworks remain fit for purpose and that their financial crime policies and procedures are effectively monitored and enforced. Businesses should also take heed of the ever-increasing extra-territorial effect of a number of tools at the disposal of HMRC.

OFFICE OF FINANCIAL SANCTIONS IMPLEMENTATION

The Office of Financial Sanctions Implementation (OFSI) sits within HM Treasury and is responsible for implementing and enforcing financial sanctions in the U.K. Although the U.K. is able to impose sanctions of its own volition in certain circumstances, the vast majority of OFSI's work is focused on implementing and enforcing sanctions imposed by the United Nations (UN) and the European Union.

OFSI was created in 2016 with the aim of enabling financial sanctions "to make the fullest possible contribution to the U.K.'s foreign policy and national security goals." OFSI's work is also viewed as a key component in the U.K.'s efforts to maintain confidence in, and the integrity of, the financial services sector.

In its Mutual Evaluation of the U.K.'s anti-money laundering and counter-terrorist financing measures, published in December 2018, the Financial Action Task Force (FATF) recognized the creation of the Office as bolstering the U.K.'s "commitment to the robust implementation and enforcement of financial sanctions." The U.K.'s commitment was underlined by a significant increase in OFSI's funding in 2018, facilitating a staffing increase of 20% and the creation of two new teams; a litigation branch and an international engagement branch tasked with improving collective global enforcement of financial sanctions. The funding increase, at a time when most U.K. Government departments' budgets were being cut or frozen, is a clear indication of the Government's continued commitment to building an effective sanctions regime in the post-Brexit era.

KEY DEVELOPMENTS

In October 2019, OFSI published its annual review covering the period from 1 April 2018 until 31 March 2019. As at 31 March 2019, 32 financial sanctions regimes were in force – an increase of three compared to the previous year. Those regimes in force related to Afghanistan, Belarus, Libya, Iran, Syria and Turkey, among others. A full list of the financial sanctions regimes currently in force is published by OFSI.

The three new regimes introduced during the annual review period related to:

- Myanmar, or Burma, in April 2018: this regime consists of an arms embargo, export controls, asset freezes and travel bans. The regime targets local security forces who commit human right violations.
- The Republic of Maldives in July 2018: this regime, which has since been terminated, consisted of travel bans and asset freezes against individuals in the country responsible for human right violations and who undermined the rule of law.
- The Chemical Weapons regime in October 2018: this regime consists of asset freezes and travel bans, and is intended to deter the proliferation and use of chemical weapons.

The Maldives regime was terminated on 17 June 2019 due to an improving political climate. Announcing the repeal, the European Council noted that "the holding of peaceful and democratic parliamentary elections on 6 April 2019 was a welcome step. The government confirmed its firm commitment to consolidate democracy, ensure good governance, and promote respect for human rights..."

As at 31 March 2019, 2,183 individuals and entities were subject to an asset freeze under 28 different regimes. Those individuals and entities now appear on OFSI's Consolidated Search List—a composite list of targets across all financial sanction regimes implemented in the U.K. who are subject to an asset freeze and/or investment bank—to help businesses carry out due diligence effectively. A further 40 targets were added to the list between 2018 and 2019, taking the total number of targets to 162. The additional targets were identified across several regimes, with a quarter being identified under the regime applying to the Democratic People's Republic of Korea (DPRK) and a fifth identified for undermining Ukrainian sovereignty.

A key development for businesses to note is OFSI's introduction of threat-specific regimes rather than country-specific regimes. For example, a cyber-attacks regime was implemented in June 2019, following on from the introduction of the Chemical Weapons regime in October 2018. The cyber-attack regime is intended to target individuals and entities responsible for conducting large-scale cyber-attacks that threaten the integrity, security and economic competitiveness of the EU. The regulation enables OFSI to impose a travel ban and asset freezes against any person or entity responsible for conducting a cyber-attack; defined as any unauthorized or illegal access to information systems, information systems interference, data interference or data interception. To impose the sanction, the attack must threaten the interests of the EU or its Member States.

Financial sanctions continue to play a key role in combating terrorist financing activities. In the period from April 2018 to March 2019, HM Treasury, who has

overall responsibility for implementing financial sanctions, renewed (on instruction from the UN) designations of 19 individuals and entities, and delisted one individual in accordance with other U.K. counter-terrorism legislation. Businesses should note that counter-terrorism regimes do, in part, operate slightly differently to the financial sanctions regimes listed above. In most circumstances, the UN has overall responsibility for enforcement and designations and HM Treasury, through OFSI, is responsible for licensing and compliance with the regime in the U.K. This structure is set-up by various pieces of legislation, including the ISIL (Da'esh) and Al-Qaida (Asset-Freezing) Regulations 2011 and the Terrorist Asset Freezing Act 2010. A further difference arises under the 2010 Act that allows the U.K. Government to unilaterally identify terrorist organizations and impose sanctions against such entities.

REPORTING BREACHES

Between 2018 and 2019, OFSI received 99 reports of suspected breaches amounting to a value of £262 million. Of the reported breaches, OFSI observed:

- an increase in reported breaches under the Libya and the Iran (Human Rights) sanction regimes;
- a decrease in reported breaches under the Iran (Nuclear Proliferation) regime;
- an increase in the value of breaches reported under the DPRK and Iran regimes; and
- an increase in the value of reported breaches for sanctions regimes involving Russia but a decrease in the number of breaches reported concerning Russian regimes.

Both the number and value of reported breaches in the period from April 2018 to March 2019 is lower than the previous year. Nevertheless, OFSI did not identify any obvious trends that evidenced a suppression in reporting.

ASSET FREEZING

Asset freezing is OFSI's standard method of compliance and enforcement. As of September 2018, £11.9 billion of frozen funds were held by U.K. businesses.

MONETARY PENALTIES

2019 saw OFSI use civil monetary penalties as a method of enforcement for the first time.

Two of these penalties came under the EU's Egypt financial sanctions regime. The first penalty was made on 21 January 2019 against Raphael & Sons plc, a small independent bank based in the U.K. The Bank transacted with funds belonging to a person designated under the Egypt financial regime amounting to £200 without a license. The Bank disclosed the transaction to OFSI when it became aware of the infringement. OFSI concluded that a penalty of £10,000 was reasonable and proportionate in the circumstances. However, as the Bank made a voluntarily disclosure and cooperated during investigations, OFSI reduced the penalty by 50% to £5,000.

The second monetary penalty was imposed on 8 March 2019 against Travelex U.K. Ltd (Travelex) under the same Egyptian regime. Travelex, a foreign exchange specialist, was issued with a £10,000 fine for transacting with funds belonging to a designated person. The transaction was valued at £204. In explaining its decision to issue a monetary penalty, OFSI stressed that "no matter the value of the transaction, the breach directly contravened the policy intention of the asset freeze." Travelex's actions allowed the designated person to utilize funds which should have been frozen. Unlike Raphael & Sons plc, Travelex was not granted a discount for voluntary disclosure.

The third and largest monetary penalty imposed by OFSI, was made on 9 September 2019 against Telia Carrier U.K. Limited (Telia Carrier), a telecommunications provider. Telia Carrier was fined £146,341 for multiple breaches of the U.K.'s Syrian sanctions regime. The company had, through its telecommunications services, indirectly provided access to funds and other economic resources to a designated entity, SyriaTel. This fine replaced the earlier penalty of £300,000 which was imposed earlier in the year, but which was altered following a ministerial review. Whilst the Minister concluded that OFSI's decision was reasonable and proportionate in the circumstances, taking further material and clarifications into consideration, the Minister reduced the penalty to £146,341. Telia Carrier did not make any voluntary disclosures.

Readers may take the view that, to date, OFSI's enforcement activity has been relatively lackluster. It will be interesting to see what outcomes OFSI delivers in 2020.

LICENSING

To maintain financial stability, OFSI has the power to award individuals and entities licenses and authorizations to conduct certain financial activity in countries that would otherwise be prohibited under a sanctions regime.

Between April 2018 and March 2019, OFSI issued 58 new licenses and made 84 license amendments. Of the 58 new licenses, half of these were to allow the payment of legal fees. The number of licenses relating to the Libya regime almost doubled to 30.

LOOKING AHEAD

In recent years, OFSI, along with various other U.K. Government departments and agencies, has been working to develop an autonomous sanctions framework ahead of the U.K.'s withdrawal from the EU, which took place on 31 January 2020. Whilst OFSI intends to largely replicate the EU's legislative framework concerning financial sanctions, there are a number of key issues for OFSI to grapple with.

From what we know so far, OFSI is unlikely to make any immediate changes to the sanctions regimes that were in force prior to withdrawal. These "static" regimes were "carried over" upon the U.K.'s withdrawal on 31 January 2020. However, for regimes which are seen as extremely important to furthering the U.K.'s foreign policy objectives, the U.K. Government has signaled that it intends to introduce new statutory instruments dealing with those regimes. This will enable it to tailor regimes in accordance with the U.K.'s national and international interests.

One of the key pieces of new legislation businesses should be aware of is the Sanctions and Anti-Money Laundering Act 2018 (SAMLA) which received royal assent on 23 May 2018 and came into effect on 31 January 2020. SAMLA grants the U.K. Government broad powers to implement and enforce financial sanctions in line with the country's foreign policy objectives.

As an example of the way in which the U.K. may look to tailor sanctions regimes in the coming months, readers should consider the Russia (Sanction) (EU Exit) Regulations 2019, which were introduced in April 2019, but will not take full effect until the conclusion of the transition period, currently scheduled to come to an end on 31 December 2020. When the Regulations do take effect, they will replace, with substantially the same effect, the relevant EU sanctions regimes.

All individuals and entities identified on OFSI's Consolidated Search List prior to withdrawal will remain listed in the short term. However, the list is subject to change and businesses should conduct a review of all high-risk parties on a regular basis to ensure effective compliance and risk-management.

Foreign Secretary Dominic Raab has signaled the U.K. Government's intention to introduce new sanctions against human rights abusers. His comments are consistent with the U.K. Government's desire to create a broad coalition of nations intent on punishing regimes that commit human right offences. The introduction of "Magnitsky legislation" will allow the Government to impose asset freezes and visa bans on torturers, murderers and corrupt officials. As readers will be aware, similar provision already exist in the U.S. and Canada.

Finally, it is important to note that the Government has faced Parliamentary scrutiny in recent months over its perceived lack of a clear sanctions strategy. A recent Select Committee report highlighted that it received "muddled answers" regarding the rolling over of EU sanctions, the introduction of Magnitsky powers and the Government's sanctions policy post-Brexit. Given the lack of clarity, businesses should pay close attention to developments in this area in the coming months.

IN-DEPTH

- AIRBUS'S RECORD-BREAKING €3.6 BILLION SETTLEMENT TO AVOID PROSECUTION
- UK'S IMPLEMENTATION OF THE EU'S FIFTH MONEY LAUNDERING DIRECTIVE
- POST-BREXIT COOPERATION IN RELATION TO CRIMINAL MATTERS

AIRBUS'S RECORD-BREAKING €3.6 BILLION SETTLEMENT TO AVOID PROSECUTION

On 31 January 2020, Airbus SE (Airbus) reached final agreements with the French Parquet National Financier (PNF), the U.K.'s Serious Fraud Office (SFO) and the U.S. Department of Justice (DoJ) in order to resolve investigations into allegations of bribery and corruption. The agreement reached with the U.S. authorities also resolves investigations by the DoJ and the State Department into inaccurate and misleading filings made by Airbus with the State Department pursuant to the International Traffic in Arms Regulations (ITAR).

Under the agreements, which are the largest ever entered into by the PNF and the SFO, Airbus will pay a total of €3.598 billion plus interest and costs to the French, U.K. and U.S. authorities to avoid prosecution. That figure equated to $3,986,888,000 and £3,021,956,000 on 31 January 2020.

This record-breaking enforcement outcome will no doubt be of interest to all corporate entities as they seek to implement, monitor and enforce anti-bribery and corruption policies and procedures. In particular, it provides further examples of the extra-territorial reach of anti-corruption legislation and the willingness of authorities in jurisdictions beyond the U.S. to embrace alternatives to immediate prosecution.

OVERVIEW

Under the agreement reached with the PNF, known as a Convention Judiciaire d'Intérêt Public (CJIP) or Judicial Public Interest Agreement, Airbus is required to pay €2,083,137,455. Airbus has also committed to submitting its compliance program to targeted audits carried out by the Agence Française Anticorruption (AFA). In return, the PNF has agreed to suspend prosecution for a period of three years.

Under the Deferred Prosecution Agreement (DPA) reached with the SFO, Airbus is required to pay €983,974,311 (£826,439,004) by way of a financial penalty and €6,989,401 (£5,870,390) in costs within 30 days. In return, the SFO has also agreed to suspend prosecution for a period of three years.

Under the DPA reached with the U.S. authorities, Airbus is required to pay €525,655,000 ($582,470,179) to the DoJ and a further €9 million ($9,972,760) to the State Department of which €4.5 million ($4,986,380) may be used for approved remedial compliance measures. In return, the U.S. authorities have agreed to suspend prosecution for a period of three years.

If Airbus complies with the terms of the agreements reached for the length of time that those agreements are in operation, the prosecutions in each jurisdiction will be discontinued. In light of the role to be performed by the AFA under the CJIP, monitors will not be imposed on Airbus under the U.K. or U.S. DPAs.

BACKGROUND

As readers will undoubtedly be aware, Airbus is one of the two largest manufacturers of commercial aircraft in the world. It also manufactures helicopters, military transports, satellites and launch vehicles. Although known by a different name at the time, the legal entity known as Airbus SE since 2017 was created by the merger of three European aerospace and defense companies in 2000. It was converted into a European public-limited company in 2015.

The turnover for Airbus SE for the years 2011 to 2018 ranged from €49 billion to €66.5 billion. Its profits before finance costs and income taxes for the same period ranged from €1.5 billion to €5 billion, which puts into context the scale of the financial settlement reached.

Airbus operates in a variety of markets and geographical areas using a number of subsidiaries. Although much of the conduct covered by the agreements relate to the activities of those subsidiaries or those acting at their request, Airbus SE, as the parent company, is the only party to the settlement agreements.

The various investigations centered on Airbus's use of "business partners"—third parties who were used to increase Airbus's international footprint and to assist in winning sales contracts.

In 2012, Airbus commissioned a private company to review its compliance program and was awarded an "anti-corruption certificate." At this time, Airbus also had a number of written policies governing payments to, and contractual relationships with, third parties. These policies were specifically aimed at ensuring that third parties were used appropriately and only after sufficient due diligence had been undertaken.

In September 2014, Airbus initiated a review of all third-party relationships. An internal report found material breaches of compliance procedures. This led to a freeze on all payments to business partners and international

market development projects. A subsequent review led to a restructuring of the legal and compliance functions within the business, and, in April 2015, Airbus published new rules regarding future third-party engagements.

INVESTIGATIONS

As part of its business, Airbus obtained export credit financing from export credit agencies, including U.K. Export Finance (UKEF)—a U.K. Government body. In April 2015, UKEF wrote to Airbus regarding UKEF's anti-bribery procedures and made specific reference to UKEF's obligations to report all suspicious circumstances to the SFO.

In late 2015, Airbus conducted a review of the accuracy and completeness of its declarations relating to its use of business partners in applications for export credit financing, and first reported its concerns to UKEF in January 2016. Both UKEF and Airbus reported matters to the SFO on 1 April 2016.

On 15 July 2016, the SFO formally opened a criminal investigation against Airbus and associated persons. Airbus was notified of this on 5 August 2016 and promptly informed the financial markets.

On 31 January 2017, the SFO and the PNF entered into a Joint Investigation Team (JIT). The JIT's investigation was vast in scale and scope. It covered all of the business partners engaged by Airbus until 2016—more than 1,750 across the globe—although the JIT decided to focus on relationships with 110. The PNF and SFO divided up the conduct under investigation between them by country.

By the end of 2018, the U.S. authorities were also investigating Airbus.

CONDUCT

According to court documents, beginning in at least 2008 and continuing until at least 2015, Airbus engaged in and facilitated a scheme to offer and pay bribes to decision-makers and other influencers, including to foreign officials, in order to obtain improper business advantages and to win business.

In France, the U.K. and the U.S., specific examples of Airbus's conduct were presented in order to demonstrate the allegations made against Airbus. It is certainly not the case that the authorities have alleged, or that Airbus has accepted, that its use of business partners, generally, facilitated the payment of bribes in all or even most cases.

The underlying facts have been described in some quarters as "eyebrow-raising." In one instance, Airbus paid $50 million in sponsorship to a sports team owned by airline executives to help win a contract for 180 aircraft. In another, the wife of an airline executive was used as a consultant on an aircraft contract despite her having no experience in aviation. Airbus later misled the UKEF about her identity when it was applying for assistance in funding the deal.

FRENCH PERSPECTIVE

The financial settlement reached under the CJIP is the largest ever and dwarfs the €500 million public interest fine, or amende d'intérêt public, imposed against Google subsidiaries in September 2019 to settle a PNF tax investigation. It comprises the disgorgement of Airbus's tainted profits of €1,053,377,113 and an additional penalty of €1,029,760,342. The latter additional penalty was calculated based on the application of a 50% discount rate from the original amount, which the Court applied as a result of inter alia "the exemplary level of cooperation with the JIT investigations." The fine that Airbus agreed to pay as part of the DPA entered into with the U.S. authorities was also deducted.

It is the tenth CJIP entered into since they were introduced under the French anti-corruption law commonly referred to as Sapin II, which was enacted on 9 December 2016. It is the sixth CJIP entered into by the PNF.

A CJIP may be offered to any legal person under suspicion or investigation for offenses related to corruption in situations in which it appears in line with the public interest not to initiate a criminal prosecution. Any agreement may include the payment of a public interest fine (limited to 30% of the company's average annual turnover), the implementation of a compliance program under the supervision of the AFA and/or the payment of compensation to victims who have suffered a loss.

Any CJIP agreed between the parties is subject to validation by the Tribunal Judiciaire, which controls (i) whether it is appropriate to use this process, (ii) whether all procedural rules have been complied with and (iii) whether the amount of the fine is within the limits prescribed by Article 41-1-2 of the French Criminal Code and is proportional in light of the profits the company derived from its wrongdoing.

The CJIP reached with Airbus confirms the determination of the French authorities to tackle corruption and an increasing willingness to pursue major international corporations. It also highlights the significant benefits that a corporation can obtain by fully cooperating during the course of an investigation,

re-affirming the guidance issued by the PNF and AFA in June 2019. In addition, the AFA concluded that the work carried out by Airbus between 2015 and 2019 to implement corrective measures at an early stage to prevent reoccurrence was of the highest standards in the field. These factors weighed heavily in favor of validation of the CJIP and in the reduction of the fine.

UK PERSPECTIVE

This DPA is the seventh concluded in the U.K. since its introduction in 2014 and the fifth relating to allegations of bribery and corruption. The financial settlement is the largest ever and is significantly greater than the £497,252,645 settlement reached between the SFO and Rolls-Royce in January 2017. To put things into context, the Airbus settlement is bigger than the total value of the financial settlements concluded under all previous DPAs and double the total of all fines paid in respect of all criminal conduct in England and Wales in 2018.

Under the U.K. regime, which was introduced by the Crime and Courts Act 2013, a corporation is charged with offenses, but proceedings are suspended if the DPA is approved. Prior to the terms being agreed, the designated prosecutor must seek a declaration from the court that such an agreement is likely to be in the interests of justice. Such a hearing takes place in private.

Having provided such a declaration on 28 January 2020, the President of the Queen's Bench Division of the High Court, Dame Victoria Sharp, approved the DPA at a public hearing on 31 January 2020. Its terms are those that lawyers in the U.K. have become familiar with (e.g., payment of a financial penalty and costs, a duty to cooperate as part of the SFO's ongoing investigations, etc.). The financial settlement comprises disgorgement of €585,939,740 and a financial penalty of €398,034,571—the latter being reduced by 50% to take account of Airbus's willingness to enter into such an agreement, its cooperation and its remediation efforts.

The Court concluded that while Airbus's conduct was extremely serious, the interests of justice were nevertheless served by a DPA rather than a prosecution for a number of reasons.

First, after what was described by the Judge as "a slow start," Airbus had cooperated "to the fullest extent possible." The Court noted that the company had taken an unprecedented step for a Dutch or French domiciled company by reporting conduct that had largely taken place overseas to the U.K. authorities thereby recognizing the extra-territorial effect of the Bribery Act 2010. The Court also listed the various ways in which Airbus had cooperated with the JIT investigations. The list accords with the updated guidance on corporate cooperation issued by the SFO in August 2019. Interestingly, the Court highlighted that Airbus had adopted a "cooperative position in respect of privilege," which has been a significant issue in recent SFO investigations. Like her French counterpart, the Judge concluded that the level of cooperation was "exemplary."

Second, the Court highlighted the implementation of a number of measures that have "transformed Airbus into what is, for present purposes (in relation to issues of compliance, culture and the like) effectively a different company." In addition to the changes to its compliance program and an overhaul of its corporate governance structures, the Court noted the appointment of a new CEO, CFO and General Counsel.

Third, the Court considered the collateral effects of prosecution and conviction. The Court noted that there are limits as to how far such matters can be taken into account and that "no company is too big to prosecute." However, factors such as the long-term effects on the viability of a business and potential debarment from tendering for public sector contracts may be relevant. The efficient use of public resources will also be a factor to take into account.

US PERSPECTIVE

DPAs have been a feature of the U.S. criminal justice system for longer than they have in France or the U.K. While they must be approved by a court, U.S. judges have traditionally played less of an active role in scrutinizing them than their French and British counterparts, with the parties being given greater leeway to resolve the terms of any agreement between themselves.

The DPA with the DoJ focused solely on a bribery scheme in China. Indeed, the DoJ acknowledged the limited reach of its jurisdiction over Airbus, explaining, "the Company is neither a U.S. issuer nor a domestic concern, and the territorial jurisdiction over the corrupt conduct is limited." However, despite covering only one jurisdiction and recognizing the stronger claim of the French and U.K. authorities, the DoJ still levied a significant penalty against Airbus.

Under the DPA, the total penalty for the alleged conduct in breach of the Foreign Corrupt Practices Act (FCPA) would have been nearly $2.1 billion. However, the DoJ agreed to credit Airbus with $1.8 billion for the sums to be paid to the PNF. The DoJ also awarded Airbus with a 25% discount for full cooperation and remediation—significantly less than that provided by the French and

English courts. Notably, the DoJ did not award voluntary disclosure credit to Airbus since it disclosed the conduct "after the corruption-related investigation being undertaken by [the SFO] in the United Kingdom began and was made public." The DoJ did note that Airbus "did disclose the conduct to the Fraud Section within a reasonably prompt time of becoming aware of corruption-related conduct that might have a connection to the United States."

The DoJ's position regarding voluntary disclosure provides companies with some insight into an issue that has been somewhat ambiguous based on the DoJ's guidance, but it also raises an interesting conundrum. The FCPA Corporate Enforcement Policy requires companies to provide information to the DoJ "prior to an imminent threat of disclosure or government investigation." The DoJ guidance does not specify that an investigation of any corrupt conduct, including in a foreign country for foreign conduct, could foreclose a company from receiving voluntary disclosure credit in the U.S. Therefore, after Airbus, to preserve voluntary disclosure credit, and the possibility of a declination, companies will need to decide whether to disclose to U.S. authorities conduct with no U.S. ties, in case such ties are later discovered in the course of an ongoing investigation. Paired with the DoJ's emphasis on timely disclosure, this may prove particularly challenging in practice.

Another noteworthy aspect of the U.S. enforcement action is that the State Department joined the DoJ in order to resolve alleged violations of the Arms Export Control Act and its implementing regulations, the ITAR. These export controls came into play because Airbus provides "defense articles" and "defense services," which are covered by ITAR regulations (i) prohibiting the payment of "political contributions, fees, and commissions" in connection with ITAR-covered products without reporting them and (ii) failing to maintain proper records of the sale of these products. The charges made by the State Department cover a larger number of countries, including Ghana, Indonesia and Vietnam.

The involvement of the State Department in an enforcement action against a foreign corporation for corruption-related offenses is quite rare, but recently there has been an increasing overlap between the FCPA and the economic sanctions regime in the U.S. Indeed, in 2019, the U.S. Securities and Exchange Commission brought an enforcement action against Quad/Graphics for alleged violations of the FCPA, economic sanctions and export control laws for engaging in transactions with Cuba. Further, some recent U.S. sanctions regimes have focused on targeting individuals allegedly involved in corrupt activities. Compared to the FCPA, economic sanctions imposed by the U.S. potentially have a much wider application and might be able to allow the U.S. to tackle corrupt conduct beyond the reach of the FCPA.

KEY TAKEAWAYS

This outcome has been widely recognized as one of the most important in the field of corporate crime in recent years. Here are the key takeaways:

- The role of UKEF, in this case, highlights that government and quasi-government bodies who do business with corporations will be keeping a close eye on their anti-corruption measures. A corporation with insufficient or ineffective anti-corruption measures is likely to find it increasingly difficult to create and maintain such relationships.
- It is also important to remember that such bodies operate policies that require them to report any causes for concern to the relevant authorities.
- While the financial costs of reaching such settlements may be significant, the advantages to a corporate entity in doing so remain obvious.
- Similarly, settlements remain an attractive way of resolving investigations for authorities with limited resources that are under increasing pressure to deliver timely outcomes.
- No matter how serious the underlying conduct, a corporate entity may still avoid prosecution if the other factors that weigh in favor of a DPA are present.
- When to self-report and to whom, remain the key decisions that any corporate entity who has uncovered wrongdoing will be required to make. These decisions can have significant consequences on the outcome that may be achieved at a later date.
- Enforcement agencies and those approving DPAs remain keen on incentivizing timely self-reporting and meaningful cooperation. Recent outcomes suggest that this is likely to be a key factor in whether a DPA is offered or approved.
- Authorities will not necessarily accept the results of an internal investigation. In the Airbus case, the JIT carried out extensive investigations in order to interrogate and validate the company's narrative.
- The implementation of remedial measures and cultural changes after wrongdoing has been discovered will also be an important factor in determining whether to offer or approve a DPA. Changes in personnel can be significant, but those responsible for making such decisions will be looking for much more than that.
- The consequences for a corporate entity of prosecution and conviction appear to be less important when considering whether to offer or approve a DPA. In France, the U.K. and the U.S., the

authorities subscribe to the view that no company is too big to prosecute.

- There is more cooperation between investigation and prosecution agencies than ever before. In this case, such cooperation extended far beyond France, the U.K. and the U.S. to virtually every continent in which Airbus carried on business.
- Equally, authorities are getting far better at coordinating their efforts to reach simultaneous outcomes.

UK'S IMPLEMENTATION OF THE EU'S FIFTH MONEY LAUNDERING DIRECTIVE

U.K. revisions to its anti-money laundering and counter-terrorist financing regime came into force on 10 January 2020.

The U.K.'s revisions implement the European Union's Fifth Anti-Money Laundering Directive, commonly referred to as "5MLD" and are designed to strengthen the U.K.'s AML and CTF regimes in order to meet the Financial Action Task Force's (FATF) global standards. The U.K. has opted to go further than certain of the EU's requirements, indicating that it intends to continue in its position as a leading global financial center, and its strict regulation and enforcement of the AML and CTF regimes.

EU Member States were required to implement the provisions set out in 5MLD by 10 January 2020. Therefore, even though the U.K. left the EU on 31 January 2020, as a Member State on the implementation date, it was required to transpose the provisions of the Directive into domestic law.

MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT) REGULATIONS 2019

On 20 December 2019, the U.K. Government published the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (the 2019 Regulations), the statutory instrument that gave effect to most of the legislative changes required under 5MLD. The 2019 Regulations amend the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the 2017 Regulations)—the domestic legislation that gave effect to the EU's Fourth Anti-Money Laundering Directive in the U.K. These laws require companies to know their customers and to manage the risks of AML/CTF.

The 2019 Regulations impact the U.K.'s AML and CTF regimes in a number of ways, including:

- extending the scope of persons subject to the 2017 Regulations;
- extending customer due diligence measures;
- creating bank account portals to be accessed by financial intelligence units (FIUs) and national regulators; and
- creating a system of registration for crypto-asset businesses.

The majority of the provisions set out under the 2019 Regulations came into force on 10 January 2020, with the exception of those governing customer due diligence on anonymous prepaid cards and requests for information about accounts and safe-deposit boxes, which will come into force on 10 July and 10 September 2020, respectively.

The 2019 Regulations take account of responses to HM Treasury's consultation on 5MLD implementation, which concluded in June 2019 (the Consultation). HM Treasury has announced that it intends to publish feedback on responses received during the Consultation in due course.

NEW PERSONS SUBJECT TO THE 2017 REGULATIONS

Under the 2019 Regulations, the scope of persons subject to the 2017 Regulations has been expanded to include crypto-asset exchange providers, custodian wallet providers and crypto-asset automated teller machines. Interestingly, the scope of the U.K.'s definition of "crypto-asset" is broader than the equivalent "virtual currency" definition laid out under 5MLD and acts as an example of the U.K.'s willingness to develop and expand the scope of the EU's rules when it considers it appropriate to do so.

The regime is also to be extended to include the letting agency sector for high-value transactions (i.e., where properties command monthly rents of €10,000 or more) and to art market participants for transactions that exceed €10,000.

The expansion of persons subject to the 2017 Regulations has been introduced in order to close perceived loopholes, in addition to taking account of advances in financial technology and changes in behavior.

In a deviation from the proposed measures published by the U.K. before the Consultation, publishers of open-source software and non-custodian wallet providers will not fall within the scope of the 2017 Regulations.

CUSTOMER DUE DILIGENCE

Under the changes introduced by the 2019 Regulations, letting agency businesses and art market participants, as well as crypto-asset exchange providers and custodian wallet providers, will be required to apply customer due diligence measures (subject to existing *de minimis* thresholds), together with all other obligations under the amended 2017 Regulations.

In line with recent changes to FATF standards, the 2019 Regulations also enhance the stringency of due diligence requirements, requiring relevant individuals to take reasonable measures to understand the control structure and ownership of their clients and to verify the identities of managing officials where beneficial ownership of a corporate entity is unclear.

Those subject to the 2019 Regulations are also required to carry out enhanced customer due diligence if they have a business relationship with a person established in a high-risk third country or in relation to any relevant transaction where any of the parties is established in a high-risk third country. The EU is responsible for designating a country as "high-risk" and maintaining the so-called "blacklist." However, as readers may be aware, there has been some disagreement between Member States in recent months over which countries should be designated as "high-risk."

BANK ACCOUNT PORTALS

Under the 2019 Regulations, FIUs and national regulators must be given access to details about U.K. bank accounts, building society accounts and safe deposit boxes for certain specified purposes, including where a national crime agency is carrying out its FIU functions, or any other law enforcement authority is investigating money laundering, terrorism or carrying out its supervisory functions. In practice, this means authorities will be able to obtain details, such as account IBAN numbers, dates of the opening and closing of accounts and the names, dates of birth and addresses of relevant account holders and beneficial owners. The intention is to improve the effectiveness of those tasked with investigating and regulating the AML and CTF regimes.

CRYPTO-ASSET BUSINESSES

As can be seen from the measures set out above, the U.K. implementation of 5MLD seeks to strengthen the AML/CTF regulation of crypto-assets. The 2019 Regulations also appoint the U.K.'s Financial Conduct Authority (FCA) as the supervisor of U.K. crypto-asset businesses for AML/CTF purposes. The FCA has published information on the scope of the activities caught by the 2019 Regulations and how entities should obtain registration, as well as its approach to supervision of crypto-asset businesses. Registration with the FCA for AML/CTF purposes is not equivalent to a firm obtaining authorization to conduct regulated activities in the U.K. and the FCA has warned crypto-asset businesses not to mislead their customers as to their status and any protections that may apply.

Under the 2019 Regulations, new crypto-asset businesses are required to have registered with the FCA before they can conduct crypto-asset activities. Crypto-asset businesses that are already operating in the U.K. prior to 10 January 2020, will be afforded a transitional period until 10 January 2021 in which to register. To be registered, a crypto-asset business must demonstrate that it, and its owners and senior managers or officials, are "fit and proper." However, the FCA has confirmed that regardless of registration it will begin the supervision of in-scope crypto-asset businesses on 10 January 2020. Those businesses that pose the highest money laundering and terrorist financing risk are likely to be subject to an enhanced supervisory focus. Crypto-asset exchange providers and custodian wallet providers must comply with certain reporting requirements and the FCA will maintain a register of such entities.

The 2019 Regulations follow a policy statement and guidance issued by the FCA in June 2019 on when crypto-assets will fall within the U.K. regulatory perimeter. Those publications made clear that certain crypto-asset activities, including the issuance of e-money tokens or use of tokens to facilitate regulated payment services, may well fall within the FCA's existing regulatory ambit and that such activities are expected to become an accepted aspect of the U.K. financial system going forward. HM Treasury is considering whether to expand the FCA's regulatory perimeter to capture more crypto-asset business. The FCA's enhanced focus on crypto-asset money laundering risks reflects a growing international concern with the increased use of crypto-assets.

AML AND CTF POST-BREXIT

The potential for the U.K. to deviate from the EU's legal and regulatory frameworks in the post-Brexit era has been a topic of much debate in recent years. However, all indications suggest that the U.K. is unlikely to reduce the AML and CTF measures to be applied by those subject to the 2017 Regulations following withdrawal from the EU.

Of course, until the conclusion of the transition period, which is currently scheduled to come to an end on 31 December 2020, most EU laws, including those

concerning AML and CTF will continue to apply. Therefore, the U.K. must adhere to the current EU standards, as well as any further EU legislation that may come into effect in this area for at least the next few months. Thereafter, the scope for divergence will depend on the nature of the U.K.'s future relationship with the EU.

Article 82 of the revised Political Declaration published in October 2019, which sets out the U.K. and EU's intentions for their future relationship, states that it should cover arrangements for cooperation in "anti-money laundering and counter terrorism financing." Article 89 states that the U.K. and EU also agree "to support international efforts to prevent and fight against money laundering and terrorist financing, particularly through compliance with [FATF] standards and associated cooperation."

At present, the Political Declaration is merely a list of aspirations. Nevertheless, even when there remained the chance that the U.K. would leave the EU without reaching any form of agreement, HM Treasury publicly committed to transposing 5MLD regardless of whether the U.K. was a Member State on the date of implementation. Indeed, the Explanatory Memorandum to the 2019 Regulations states that "as a leading member of the FATF, the U.K. will continue updating anti-money laundering policies according to international standards, ensuring the U.K.'s AML/CTF regime is kept up to date, effective and proportionate."

Further revisions to international AML/CTF standards are expected in the coming years. In December 2019, the Council of the EU adopted strategic priorities for further reforms to the EU's AML/CTF regime and has requested that the European Commission take action to put those priorities into effect. A report on the European Commission's progress is expected in June 2020. The EU also shares the concerns expressed by international bodies that global "stablecoin" projects should be subject to appropriate regulatory frameworks, and that money laundering and terrorist financing risks are among the issues to be addressed.

Therefore, as matters currently stand, where the EU introduces further legislation to implement FATF or other globally recognized standards, the U.K. is likely to remain in close alignment and as the 2019 Regulations demonstrate, in some areas, may well go further.

POST-BREXIT COOPERATION IN RELATION TO CRIMINAL MATTERS

In 2019, the House of Commons Library stated that the U.K. participated in approximately 40 EU measures that aimed to support and enhance internal security and policing, and judicial cooperation in criminal matters. Those measures cover a broad range of areas that have helped the U.K. forge deep and long-lasting relationships with EU partners over the years, and it is widely acknowledged that Member States have always viewed the U.K. as a "key player" in this area.

Of course, although the U.K. left the EU on 31 January 2010, the Withdrawal Agreement concluded between the U.K. and the EU ensures that the Parties will continue to enjoy many of the benefits of the pre-withdrawal cooperation arrangements until the conclusion of the transition period, which is currently scheduled to end on 31 December 2020. However, what is not yet known, is the scope of the future relationship between the Parties in this area and how it will affect the day-to-day business of intelligence agencies, law enforcement bodies, prosecuting authorities and the criminal justice systems here in the U.K. and throughout the EU.

In the Political Declaration, which sets out the Parties ambitions for their future relationship, the U.K. and EU agree to provide for "comprehensive, close, balanced and reciprocal law enforcement and judicial cooperation in criminal matters, with the view to delivering strong operational capabilities for the purposes of the prevention, investigation, detection and prosecution of criminal offences, taking into account the geographic proximity, shared and evolving threats the Parties face, the mutual benefits to the safety and security of their citizens, and the fact that the United Kingdom will be a non-Schengen third country that does not provide for the free movement of persons" (see article 80).

It appears, therefore, that in this area at least, both the U.K. and the EU recognize the benefits of remaining closely integrated in order to tackle serious and organized crime, and particularly those offenses that frequently straddle borders, such as terrorism, money laundering, corruption, human trafficking and drug smuggling. The challenge will be developing mechanisms that facilitate such close cooperation between Member States and the U.K.—now a non-Member State or "third country."

Below, we discuss some of the cooperation measures that are likely to be of most interest to our readers.

EUROPEAN ARREST WARRANTS

The European Arrest Warrant, or EAW as it is commonly referred to, is a simplified cross-border judicial surrender procedure for the purpose of prosecuting or executing a custodial sentence or detention order. Under the arrangement, a warrant issued by the judicial authority of one Member State is valid throughout the entire territory of the EU and countries can only refuse to surrender a requested person on very limited grounds.

The most recent data compiled by the National Crime Agency shows that between 2015 and 2018, 48,133 requests were received from Member States for individuals believed to be in the U.K., 5,290 requested persons were arrested and 3,688 of them were surrendered to the requesting Member State. In the same period, the U.K. issued 882 EAWs, which led to 566 arrests and 482 requested persons being surrendered.

While the EAW regime has faced some criticism in the U.K., it is widely acknowledged that it has greatly assisted Member States' ability to apprehend those accused or convicted of serious wrongdoing in a timely manner and has gone a long way in helping the EU tackle cross-border crime in particular. It is unsurprising, therefore, that there has been much speculation about how the U.K. and the EU will continue to facilitate the transfer of alleged and convicted criminals expeditiously now that the U.K. is no longer a Member State.

Article 62.1(b) of the Withdrawal Agreement states that where the requested person is arrested for the purposes of the execution of an EAW before the end of the transition period, Council Framework Decision 2002/584/JHA shall apply. In effect, as long as a requested person is arrested by 31 December 2020, it will be business as usual. Interestingly, the U.K. and EU have decided to use the point of arrest as the relevant point in time rather than the date of issue or receipt of the EAW, or any other notable event. Article 612.1(b) explicitly states that the decision of the executing judicial authority as to whether the requested person is to remain in detention or be provisionally released is irrelevant for these purposes.

In November 2018, in a preliminary ruling issued in *Minister for Justice and Equality v Republic of Ireland* (C-327/18), the European Court of Justice (ECJ) refused to uphold the decision of the Irish High Court not to surrender a requested person under EAWs issued by

the U.K. The High Court had ruled that fulfilling such a request may lead to the requested person's detention at a time when the U.K. was no longer a Member State and that the rights afforded to him under EU law may not be protected and honored as a result. In rejecting such a view, the ECJ noted that the rights afforded to EU citizens were also afforded to those in the U.K. under domestic law and that there was nothing to suggest that the U.K. intended to depart from its wider treaty obligations, such as those under the European Convention on Human Rights.

What is not yet known is what the arrangements will be once the transition period comes to an end. However, article 84 of the Political Declaration states that "the Parties should establish effective arrangements based on streamlined procedures and time limits enabling the United Kingdom and Member States to surrender suspected and convicted persons efficiently and expeditiously, with the possibilities to waive the requirement of double criminality, and to determine the applicability of these arrangements to own nationals and for political offences." At first blush, it appears that the U.K. and EU will be looking to establish arrangements that are very similar to those that operate under the EAW regime.

If an agreement is not reached by the conclusion of the transition period, the U.K. and Member States will need to fall back on extradition arrangements under pre-EU treaty obligations. As matters currently stand, this will be the case even if an EAW was issued while the U.K. remained a Member State, but the requested person was not arrested before the conclusion of the transition period.

Falling back on pre-EAW arrangements will almost certainly mean a return to slower and more cumbersome justice. Domestic laws in some Member States, such as Germany, even prevent the extradition of its nationals to countries outside the EU. We are therefore of the view that this is almost certain to be an area in which the U.K. and the EU will wish to retain close cooperation.

In order to tackle the possible effects of not participating in the EAW regime, the U.K. Government has announced its intention to introduce the Extradition (Provisional Arrest) Bill. The legislation would allow those wanted in relation to serious offenses to be arrested without a warrant and taken before a court within 24 hours of arrest if they were wanted by authorities in a "trusted country." A trusted country would be a nation in whose use of Interpol Notices and criminal justice systems the U.K. has "a high level of confidence." The U.K. Government envisages that most, if not all, EU Member States would qualify.

EUROPEAN INVESTIGATION ORDERS

Like EAWs, European Investigation Orders, commonly referred to as EIOs, were introduced in an effort to improve the obtaining and transmission of evidence between Member States in relation to criminal investigations and proceedings. The framework was introduced by EU Directive 2014/41 (EIO Directive) and implemented in the U.K. by the Criminal Justice (European Investigation Order) Regulations 2017, which came into force on July 31, 2017. All Member States, save for the Republic of Ireland and Denmark, are participating Member States under the EIO framework.

EIOs can be issued by a designated prosecutor or by a court, depending on the Member State. The powers to be exercised also have a bearing on who is the most appropriate body to issue an EIO. Generally speaking, where the power to be exercised is considered coercive (e.g., search warrant, production order etc.), the power to issue will normally lie with a court.

Once issued, the Member State will directly transfer the EIO to the executing Member State who must recognize and execute any request within prescribed time limits. Like the EAW regime, there are only limited circumstances in which a Member State can refuse to execute an EIO.

Article 62.1(l) of the Withdrawal Agreement states that where EIOs are received by the central or executing authority in a Member State before the conclusion of the transition period, the EIO Directive shall apply. This effectively means that it will be business as usual until 31 December 2020, providing any EIO issued is received by the relevant authority in a Member State on or before that date. In addition, applying the reasoning of the ECJ in *Minister for Justice and Equality v Republic of Ireland*, a Member State is unlikely to be able to refuse to execute an EIO merely because the U.K. is no longer a member of the EU if the other procedural requirements have been fulfilled.

Although the Political Declaration makes a number of references to the establishment of a security partnership that should comprise law enforcement and judicial cooperation in criminal matters, EIOs are not specifically referred to. However, under article 88, the Parties agree to "consider further arrangements appropriate to the United Kingdom's future status for practical cooperation between law enforcement authorities, and between judicial authorities in criminal matters, such as joint investigation teams, with the view to delivering capabilities that, in so far as is technically and legally possible, and considered necessary and in both Parties' interests, approximate those enabled by relevant Union mechanisms."

As matters currently stand, it appears unlikely that the U.K. will be permitted to operate within the EIO framework at the conclusion of the transition period. However, there does appear to be a genuine willingness on the part of both the U.K. and the EU to find appropriate mechanisms that will allow all parties to continue to enjoy the practical benefits of close investigative cooperation and to avoid a return to the bureaucratic and time-consuming mechanisms available under pre-EU mutual legal assistance arrangements.

OTHER COOPERATION MEASURES

Article 62.1 of the Withdrawal Agreement also sets out a broad range of provisions to allow other cooperation measures to continue to be used during the transition period. These include recognition of freezing and confiscation orders, as well as criminal conviction data sharing mechanisms. In broad terms, like EIOs, providing any order or request is received by a Member State before the conclusion of the transition period, it will be executed in accordance with existing EU legislative frameworks. Again, it remains to be seen which of the current measures are re-created under the future relationship.

Under the Withdrawal Agreement, the mechanisms that allow the U.K. to participate in Europol and Eurojust will also continue until the conclusion of the transition period. Article 62.2, for example, allows the competent U.K. authorities to continue to participate in joint investigation teams established before the conclusion of the transition period.

Article 86 of the Political Declaration states that "the Parties recognize the value in facilitating operational cooperation between the United Kingdom's and Member States' law enforcement and judicial authorities, and will therefore work together to identify the terms for the United Kingdom's cooperation via Europol and Eurojust."

Of course, under the current arrangements, several non-EU countries make use of the liaison mechanisms available via Europol and Eurojust as a result of cooperation agreements concluded between the relevant EU entity and third-party states, such as the U.S., Norway and Iceland. All indications are that the U.K. will be offered the opportunity to enter into similar cooperation agreements to permit continued cooperation at the conclusion of the transition period.

LOOKING AHEAD

During his much-publicized speech on 3 February 2020, Prime Minister Boris Johnson set out his ambitions for the future relationship between the U.K. and the EU. It included the following reference:

We will seek a pragmatic agreement on security, on protecting our citizens without trespassing on the autonomy of our respective legal systems.

The Prime Minister's comments followed a speech by Michel Barnier, the EU's Chief Negotiator, delivered on 27 January 2020 in which he stated that the EU "will deepen cross-border cooperation on security including, where possible, with the U.K. as a third country to tackle gaps in the fight against serious crime and terrorism in Europe."

Therefore, it appears that this is an area in which both the U.K. and the EU possess the will to maintain a close relationship. What remains to be seen are the ways in which such a relationship will be maintained and whether any such relationship will continue irrespective of a broader agreement on the U.K.'s future relationship with the EU.

OTHER MATTERS OF INTEREST

- ACTIVITIES OF THE INFORMATION COMMISSIONER'S OFFICE
- UK-US BILATERAL DATA ACCESS AGREEMENT SIGNED
- EU WHISTLEBLOWING DIRECTIVE
- A BAN ON TV RECORDING IN CROWN COURTS IN ENGLAND AND WALES LIFTED

ACTIVITIES OF THE INFORMATION COMMISSIONER'S OFFICE

The Information Commissioner's Office (ICO) is the U.K.'s independent body created to uphold information rights. It is sponsored by the Department for Digital, Culture, Media & Sport and has existed in one guise or another since 1984.

Although the body has existed for some time, the ICO's activities have taken on greater significance following the EU's introduction of the General Data Protection Regulation (GDPR) and the U.K.'s enactment of the Data Protection Act 2018. More recently, it hit the headlines over its investigations into the activities of Cambridge Analytica, Facebook and other connected entities. Data privacy now appears to be at the forefront of most businesses' minds in the U.K., the EU and beyond, and in our view, it should be.

Whilst indications are that the ICO is unlikely to resort to prosecuting corporate entities, as opposed to individuals, for breaches of data protection legislation in anything but the most serious cases, the size and frequency of monetary penalties issued in recent years leads us to conclude that the ICO's activities over the past 12 months warrant mention in this publication.

Commenting on the release of its Annual Report in July 2019, Elizabeth Denham, the Information Commissioner, described the previous year as an "unprecedented" one for the ICO. In that period, the ICO imposed 22 fines totaling more than £3 million for breaches of data protection legislation. It also imposed 23 monetary penalties totaling more than £2 million for breaches of the EU's Privacy and Electronic Communications Regulation, which was introduced to combat nuisance calls and texts. In the same period, the ICO also experienced an increase of nearly 50% in data protection complaints, receiving a total of 41,661. The ICO also experienced a 66% increase in the use of its helpline, chat and written advice services.

In the months since the publication of its Annual Report, the ICO has continued to be very active, announcing a number of further outcomes. However, two stand out as being of particular interest to businesses looking to manage data privacy issues.

Doorstep Dispensaree Limited

In December 2019, the ICO fined Doorstep Dispensaree Ltd, a London-based pharmaceutical company, £275,000 for failing to ensure the security of special category data. Importantly, this is the first monetary penalty imposed by the ICO under the GDPR.

The company, which supplies medicines to customers and care homes, left approximately 500,000 documents, which included names, addresses, dates of birth and medical records, and spanned a period from June 2016 to June 2018, in unsecure boxes and open to the elements outside its offices in North London. The ICO concluded that the company failed to process data in a manner that ensured appropriate security against unauthorized or unlawful processing and accidental loss, destruction or damage.

The company was also issued with an enforcement notice, which requires it to improve its data protection practices within three months.

DSG RETAIL LIMITED

In January 2020, DSG Retail Limited, the parent company of Currys PC World and Dixons Travel, was fined £500,000 by the ICO after a "point of sale" computer system (i.e., that used to operate shop floor tills) was compromised by a cyber-attack.

The ICO found that the attacker had installed malware on 5,360 tills across various Currys PC World and Dixons Travel stores around the country between July 2017 and April 2018. As a result, the attacker collected the personal data of 14 million people over a nine-month period, as well as details relating to 5.6 million payment cards.

The ICO found that the company's lack of effective security systems had facilitated the attack. It was found in breach of data protection legislation by having inadequate security measures and failing to take appropriate steps to protect customers' personal data.

In January 2018, the ICO found DSG's subsidiary, Carphone Warehouse, liable for similar security breaches and imposed a penalty of £400,000.

Looking Ahead

We have little doubt that effectively handling data privacy issues will remain high on the agendas of businesses across the U.K. throughout 2020. The actions of the ICO and other international regulatory bodies tasked with enforcing data protection legislation confirms that businesses are right to take such issues seriously. Breaches of data privacy legislation not only open up businesses to potential enforcement action, but they may also lead to significant reputational damage and potential civil liabilities as well.

Two outcomes from 2019 highlight that even those tasked with enforcing the rules can fall afoul of them from time to time:

- In May 2019, HMRC was issued with an enforcement notice for failing to obtain adequate consent from around seven million individuals ahead of its collection of voice ID data through its helpline.
- In June 2019, the Metropolitan Police Service received enforcement notices for failing to comply with individuals' rights in respect of subject access requests.

UK-US BILATERAL DATA ACCESS AGREEMENT SIGNED

On 3 October 2019, the U.K. and the U.S. entered into a world-first Bilateral Data Access Agreement, which is set to accelerate the time it takes law enforcement agencies to access electronic data held by communication service providers and other relevant technology companies.

Historically, the U.K. and the U.S., amongst other jurisdictions, have had to submit an information request through Mutual Legal Assistance Treaties (MLATs) to the government of the country in which the technology company is based to access data held by that company. Once submitted, the relevant government reviews the request, and, if approved, prepares an order which is then served on the technology company to permit the government to collect the data and supply it to the investigating authority. This process can take months, and in some instances years, to complete.

Under the new agreement, law enforcement agencies in the U.K. and the U.S. will be able to request a domestic court issue an order against a company in the other country. The agency can then directly serve such an order on that company. It is hoped that this important development will allow relevant data to be obtained within a matter of weeks and possibly even days in urgent cases.

This legislative development is a product of the enactment of the Crime (Overseas Production Orders) Act 2019 in the U.K. and the Clarifying Lawful Overseas Use of Data (CLOUD) Act 2018 in the U.S. Both countries introduced such measures with a view to creating coherent frameworks that sought to give due regard to due process, privacy and the rule of law.

It is important for companies to note that these new provisions will not grant law enforcement agencies access to data which:

- the agencies would not have the right under existing domestic legislation to access;
- relates to a data subject which is resident of the country in which the evidence is requested; and
- would require technology companies to decrypt data.

The expedited process is likely to cause an increase in orders served upon communication service providers in the U.K. and the U.S. It would be wise for such companies to familiarize themselves with the process under the new agreement, as well as to review their own internal policies concerning data sharing with law enforcement agencies generally to ensure compliance.

Similar legislative provisions concerning gaining access to data in other countries are expected in both the U.K. and the U.S. in the future.

EU WHISTLEBLOWING DIRECTIVE

On 7 October 2019, the European Council adopted the EU Whistleblowing Directive. The Directive is set to provide a package of measures that will offer better protection to persons who report breaches of EU law. Member States are required to transpose the Directive into domestic law by October 2021.

The U.K., which already has significant protections in place under the Public Interest Disclosure Act 1998 and the Employment Rights Act 1996, has indicated that it will not be adopting the EU Whistleblowing Directive. However, in a letter to the House of Commons European Scrutiny Committee dated 4 October 2019, the U.K.

Government committed to reflecting on its whistleblowing framework and, in particular, to legislating to introduce a requirement for employer's to be clear on the limits of non-disclosure agreements within the written statement of employment particulars.

Despite the U.K.'s position, we recommend that entities conducting business in Europe are familiar with the terms of the Directive, and review internal policies and procedures accordingly.

A BAN ON TV RECORDING IN CROWN COURTS IN ENGLAND AND WALES LIFTED

The ban on filming in the Crown Courts of England and Wales is set to be lifted by legislation that was laid before the U.K. Parliament on 16 January 2020. The passing of the Crown Court (Recording and Broadcasting) Order 2020 will permit TV cameras, for the first time, to film judges while they make their sentencing remarks in cases involving the most serious offenses.

While trials will not be filmed and TV cameras will not be permitted to film anyone else in the courtroom, such as victims and jurors, the development marks a radical change to the operation of open justice in England and Wales. It is thought that the first broadcast may be made in a matter of months.

Commenting on the new legislation, Robert Buckland, the Justice Secretary and Lord Chancellor said:

This government, alongside the judiciary, is committed to improving public understanding of our justice system and allowing cameras into the Crown Court will do just that. It will ensure our courts remain open and transparent and allow people to see justice being delivered to the most serious of offenders.

Any live broadcasts will be subject to a short time delay to minimize the risk of any breaches of reporting restrictions or other errors. It is thought that any footage will be broadcast through a Government website, as well as through conventional media channels.

Recording of the passing of sentences has been permitted in the Scottish courts since 1992. However, the first sentencing remarks were not broadcast until 2012. It remains the case that such broadcasts are rare.

CONTACTS

IF YOU WISH TO RECEIVE MORE INFORMATION ON THE TOPICS COVERED IN THIS PUBLICATION, YOU MAY CONTACT YOUR REGULAR SHEARMAN & STERLING CONTACT OR ANY OF THE FOLLOWING PEOPLE.

SUSANNA CHARLWOOD
London
T +44 20 7655 5907
susanna.charlwood
@shearman.com

BARNABAS REYNOLDS
London
T +44 20 7655 5528
barney.reynolds
@shearman.com

THOMAS DONEGAN
London
T +44 20 7655 5566
thomas.donegan
@shearman.com

SIMON LETHERMAN
London
T +44 20 7655 5139
simon.letherman
@shearman.com

SIMON DODDS
London
T +44 20 7655 5156
simon.dodds
@shearman.com

MATHEW ORR
London
T +44 20 7655 5734
mathew.orr
@shearman.com

PHILIP UROFSKY
Washington, D.C.
T +1 202 508 8060
philip.urofsky
@shearman.com

STEPHEN FISHBEIN
New York
T +1 212 848 4424
sfishbein
@shearman.com

PATRICK D. ROBBINS
San Francisco
T +1 415 616 1210
probbins
@shearman.com

BRIAN G. BURKE
New York/Shanghai
T +1 212 848 7140
T +86 21 6136 5000
brian.burke
@shearman.com

PAULA HOWELL ANDERSON
New York
T +1 212 848 7727
paula.anderson
@shearman.com

MARK D. LANPHER
Washington, D.C.
T +1 202 508 8120
mark.lanpher
@shearman.com

CHRISTOPHER L. LAVIGNE
New York
T +1 212 848 4432
christopher.lavigne
@shearman.com

MASAHISA IKEDA
Tokyo
T +81 3 5251 1601
mikeda
@shearman.com

DANFORTH NEWCOMB
New York
T +1 212 848 4184
dnewcomb
@shearman.com


Shearman
SHEARMAN & STERLING