Contents

- Anti-money laundering and proceeds of crime  4
- Taxation  17
- Market offences  19
- Bribery and corruption  22
- Prosecutor attitudes and resources  27
- Settlement  34
- Cybercrime  35
- Sanctions  35
- Competition  36
- Other developments  39
- Looking ahead  41

Overview

This edition covers a significant number of financial crime developments from across Europe and enforcement actions in many industry sectors, including pharmaceuticals, energy, TMT, manufacturing, financial services and logistics. Investigating authorities need information, and the opacity of corporate structures and the difficulty of accessing communications data from overseas communication service providers can often make this very challenging. In this regard, we see a move towards greater transparency of beneficial ownership of companies, driven by 5MLD. From the US and the EU there are efforts to make it easier for prosecutors to obtain electronic communications data from overseas communications service providers.

Looking ahead, Brexit will undoubtedly impact on AML and sanctions law and practice in the UK, and EU. We will be covering more on that once the timing becomes more certain.

CZECH REPUBLIC

- The Financial Analytical Office issued a list of risky countries and of countries subject to international sanctions for the purpose of conducting risk analysis required by the AML Act
- Criminal proceedings against physicians and representatives of pharmaceutical companies continue
- The anti-corruption department of the Office of the Government will be relocated to the Ministry of Justice
- European Commission investigates Czech Prime Minister’s interest in AGROFERT
- The Supreme State Prosecutor’s Office issued detailed guidance for legal entities on what procedures to implement in order to fulfil the criteria of the Act on Criminal Liability of Legal Entities for exempting themselves from criminal liability

FRANCE

- French FIU publishes a report on AML/CFT trends during 2017 – 2018
- A French MP and a group of French citizens file a complaint with the National Financial Prosecutor after the publication of the “Cum/ex Files”
- The French Constitutional Court rules on the constitutionality of certain dual tax and criminal sanctions
- Leading Swiss bank convicted by the Paris Criminal Court in the biggest alleged tax evasion case in French history
- Major oil and gas company suspected of corrupting foreign public officials appeared for trial at the Paris Criminal Court
- Ill-gotten gains: French NGO Sherpa files a new complaint against the Djiboutian president and his entourage
- Former French President’s campaign director placed under formal investigation for passive corruption
- European public official convicted for active corruption by the Paris Criminal Court
- Renowned French businessman pleads guilty to settle misuse of corporate assets charges, in an ongoing investigation against former presidential candidate
- Major French company is victim of CEO Fraud
- French Senate Committee adopts a draft European resolution on the extraterritoriality of American sanctions

GERMANY

- The Public Prosecutor’s Office in Munich prepares indictment of former manager of German car manufacturer
- Second attempt to commence proceedings against 2006 World Cup Officials
- Dawn raid at a German bank on suspicion of money laundering
- Chief Public Prosecutor’s Office in Frankfurt has settled an investigation against a German bank for Cum/ex transactions
- 81,000 diesel drivers might sue German car manufacturer
- German car manufacturer linked to diesel emission scandal pays a fine of EUR800 million
- Criticism of German Money Laundering Register
- EU Commission examines German Money Laundering Special Unit
- Transactions with ADRs under review by German authorities
- Trading Bitcoin not subject to authorisation according to Berlin court

NETHERLANDS

- Potential Changes to Settlement of High-Profile Corruption Cases in the Netherlands

POLAND

- Former Chairmen of the Polish Financial Supervision Authority detained
- New rules on the responsibility of managers
Europe at a glance

ROMANIA

- More delays to Draft Law transposing 4MLD
- European Commission reports on progress towards Romanian commitments on judicial reform and the fight against corruption
- Venice Commission expresses concerns over proposed amendments to two criminal codes

SPAIN

- Proceedings against directors for accounting misrepresentations

UK

- FCA: Thematic Review: Money Laundering and Terrorist Financing Risks in the E-Money Sector
- Barrister wins right to see his bank’s suspicious activity reports
- FCA finalised guidance on financial crime systems and controls

- Nine individuals convicted in FH Bertling SFO bribery cases
- SFO Afren convictions and sentencing
- Successful conclusion to the UK’s first Deferred Prosecution Agreement
- SFO – priorities and direction outlined in a series of speeches and interviews
- Growing pressure on technology companies to disclose customer data quickly
- UK expands availability of deferred prosecution agreements
- Surveying the financial crime landscape in the UK insights across the market from the annual financial crime return
- Europol signs MoU with Diebold Nixdorf
- The future of competition enforcement in the UK

EU-WIDE

- The EU adopts its first Directive on combatting money laundering by criminal law
Anti-money laundering and proceeds of crime

EU-WIDE

First Directive on combatting money laundering by criminal law

After the adoption of 4MLD in May 2015 and 5MLD in May 2018, both relating to the civil and regulatory prevention of money laundering, the EU has adopted its first Directive aimed at combatting money laundering through the criminal law.

Directive (EU) 2018/1673 of 23 October 2018 aims to establish minimum rules harmonising the definition of money laundering offences and applicable criminal sanctions across the EU, with a view to increasing cross-border cooperation and prosecution of money laundering offenders.

The Directive requires all Member States to:

- criminalise money laundering where the conduct was committed intentionally (although the Directive insists that Member States may decide to hold offenders to a higher standard by criminalising conduct that was committed recklessly or by serious negligence – ie where the offender suspected or ought to have known that money laundering was being committed);
- criminalise self-laundering (ie allow the prosecution of the offender who is also the perpetrator of the predicate offence that generated the unlawful proceeds);
- make it unnecessary to first obtain a conviction for the predicate offence or even to establish precisely which underlying offence generated the unlawful proceeds;
- make money laundering punishable by a maximum term of imprisonment of at least four years for natural persons (along with additional sanctions and measures);
- make legal persons (eg companies) liable for money laundering offences committed for their benefit and subject to criminal or non-criminal fines and other sanctions – such as exclusion from entitlement to public benefits, aid or funding (including tender procedures, grants and concessions), disqualification from the practice of commercial activities or winding-up/closure of the entity;
- make it an aggravating circumstance:
  - for an obliged entity (ie one which is required to comply with the EU’s AML regime) to commit money laundering; or
  - to commit money laundering within the framework of a criminal organisation; and
- remove obstacles to cross-border judicial and police cooperation by setting common provisions to improve criminal investigations.

Directive 2018/1673 was published in the EU official journal of 12 November 2018 and entered into force on 2 December 2018.

Member States are free to adopt or maintain more stringent rules than those outlined above (and some already have). Those Members States which have not opted out of the criminal regime, are required to implement the minimum criminal law rules set out in the Directive by 3 December 2020.
CZECH REPUBLIC

List of high risk countries and countries subject to international sanctions issued by Czech Financial Analytical Office

Czech anti-money laundering (AML) laws require certain entities (e.g., banks, investment companies, insurance companies, etc.) to conduct a regular risk analysis to assess the risk of money laundering in their business. An obliged entity is required to consider prescribed factors, including geographic risk factors. The Financial Analytical Office has now issued a list of high risk countries and a list of countries and individuals against which, international sanctions were imposed. However, both lists should be considered a minimum standard only and many entities will no doubt already be conducting a risk analysis based on the application of stricter internal policies.

FRANCE

AML/CFT trends 2017-2018

The French FIU (Tracfin) has published its 2017/2018 annual report on AML and counter-terrorist financing (CTF) risks (the Report), in line with FATF’s First Recommendation and Article 7 of the Fourth Money Laundering Directive (4MLD).

The Report is explicitly aimed at helping regulated professionals undertake AML/CFT risk assessments. It highlights that:

- as regards terrorist financing, there has been a significant increase in the number of SARs filed with Tracfin (1,379 in total, i.e. a 17% increase compared to 2016), the quantity of information received and analysed, and the number of records shared with the intelligence and judicial services (685 in total, i.e. a 73% increase compared to 2016);
- organised fraud, particularly using forged wire transfers, the Forex market, diamonds, bitcoins, and energy saving certificates, continue to cause significant financial harm;
- carbon tax fraud is still running high and constitutes a major financial issue; and
- tax issues are the main source of SARs, counting for 29% of SARs received, half of which in turn concerned concealed activities or understated business, and a third of which concerned wealth issues (undeclared donations, holding accounts or assets held abroad).

The Report contains ten recommendations which are aimed, principally, at legislators and regulators on a French and European level, including:

- strengthening coordination between public authorities and private actors seeking to detect and fight fraud committed using shell companies;
- strengthening the regulation of electronic money payment service providers, which are increasingly used in money laundering circuits, on a European level and ensuring that national regulators have the right resources to supervise them;
- updating the Ficoba database (i.e., the French bank accounts’ database) in order to ensure that it is comprehensive, and encouraging the implementation of centralised bank databases in all EU Member States under 4MLD;
- introducing the regulation of crypto assets, which carry high risks of inherent fraud and AML risks, on an international, European and national level (a bill is currently being discussed by the French Parliament);
- reinforcing cooperation with the French Financial Markets Authority, in particular with respect to crypto assets and the means of investigating behaviour undertaken on the financial markets; and clarifying the definition of politically exposed persons in French law, provided by Article R. 561-18 of the Monetary and Financial Code.
GERMANY

Dawn Raid at German bank on suspicion of money laundering

The Public Prosecutor’s Office in Frankfurt and the Federal Criminal Police Office searched a German bank in November 2018 in an investigation into suspected money laundering. Following an evaluation of the database of the so-called “offshore leaks” and “Panama Papers” available at the Federal Criminal Police Office, the bank was suspected by the authority of helping clients to set up offshore companies in tax havens. Money received from the commission of criminal offences was allegedly transferred to the bank’s account. The head of the Public Prosecutor’s office in Frankfurt am Main reported on the bank’s comprehensive cooperation. A spokesperson of the German bank stated that active support of the investigations and constructive cooperation with the authorities will continue.

Criticism of German Beneficial Ownership Register

The Federal Transparency Register for the investigation of money laundering, tax fraud and terrorist financing was intended to be a new weapon in the fight against financial crime. However, less than a year after it was launched, it has hardly been used in practice, according to an answer provided by the federal government to a parliamentary question by the Green parliamentary group (Bündnis 90 / Die Grünen).

The Transparency Register was established in 2017 to assist investigators. It stores information on the beneficial owners of German companies, associations, cooperatives and foundations. The name, date of birth, place of residence and type and scope of economic interest are stored in the database, which is administered by the Federal Ministry of Finance.

Some critics argue that it is not useful: “In its current form, the Transparency Register is above all one thing – a data dump,” said Lisa Paus, member of the Green Party (Bündnis 90 / Die Grünen). With regard to critical, really interesting cases, the register could be undermined with a few tricks. In fact, the federal government itself sees a high risk that the backers of dubious businesses will ultimately remain in the dark. “If, for example, company networks, investment companies, offshore companies or foundations are used, it is considerably more difficult to identify the beneficial owner behind them,” writes the Ministry of Finance in its reply to the parliamentary question.

EU Commission examines German Money Laundering Special Unit

According to press reports, police authorities criticized the allegedly insufficient work of the so-called Financial Intelligence Unit, and there was even talk of a “risk to Germany’s internal security”. Since responsibility for the money laundering special unit of the Federal Criminal Police Office was transferred to the German customs office, thousands of reports of suspicion, including suspected terrorist financing, have accumulated among the investigators. In parallel, similar issues have come to light in Brussels.

Sven Giegold, financial expert for the Green party in the European Parliament, has submitted an official request to the EU Commission asking that the Commission explain how it intends to ensure German compliance with the EU’s AML regime and asking it to indicate whether it is considering infringement proceedings against Germany for violation of the EU treaties.

ROMANIA

More delays to Draft Law transposing 4AML

After its adoption, the draft law has been sent back to the Parliament in order to be amended, so that it complies with the Romanian Constitution.

The implementation date for 4MLD in Romania was 26 June 2017, meaning that it is already more than one year and a half late.

The delays have been caused by the lengthy enactment procedure, which consists of a two-step parliamentary approval (one from each decisional chamber) and an a priori constitutional control.
Shortly after the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) came into force, the FCA embarked on a review of the control frameworks in place at 13 Electronic Money Institutions (EMIs). The impetus behind the review was a desire for the FCA to increase its understanding of the key risks faced by the e-money sector and the controls in place to mitigate the risks of money laundering and terrorist financing.

**What is e-money?**

E-money is broadly defined by the European Central Bank as an electronic store of monetary value on a device which can be used for making payments and which does not necessarily involve bank accounts in transactions. Prepaid cards are the obvious example of e-money, but there is also no need for a physical product; entirely web-based payments services also constitute e-money.

**What's the risk?**

E-money products attract a heightened risk of money laundering and terrorist financing for a few reasons:

- The requirements to conduct customer due diligence in respect of e-money users are not as stringent as in respect of many traditional banking products, meaning that many products can be obtained anonymously, and by multiple ‘cardholders’.
- Many products do not have a limit on usage, or the monetary value which can be ‘loaded’ onto them.
- Use of agents and distributors (Programme Managers (PMs)) to distribute products may lead to potential outsourcing risks, such as poor governance and oversight.

**The FCA’s Findings**

The review focused on e-money products, including prepaid cards and digital wallets. The scope of the review excluded other services (such as money remittance) and activities outside of the FCA's supervisory remit (including gift cards that can be used only within a limited network, or any prepaid product denominated in a virtual currency).

**Governance, culture and management information**

Generally the FCA found that the EMIs exhibited “a positive culture and a good awareness and understanding of their financial crime obligations”. The formality and scale of the systems used to escalate and manage the risks depended on the relative size of the EMI, but the FCA considered this did not seem to impact on the effectiveness of the systems. Most EMIs produced monthly or quarterly management information reports, a practice viewed positively by the FCA.

**Risk Assessment**

Most EMIs had a comprehensive “business-wide risk assessment” in place to identify risks, but the appropriate control measures were not always implemented. Risks documented included factors such as card usage in high-risk countries and the use of PMs to distribute products. For “customer risk assessment”, the FCA found all EMIs were screening for Politically Exposed Persons (PEPs) and sanctioned individuals. However, the FCA noted that the risk tools to calculate individual customer risk were not always used effectively to trigger enhanced due diligence (EDD) and ongoing monitoring.

**Customer Due Diligence (CDD) and EDD**

For CDD, all EMIs were identifying and verifying customers in accordance with the MLRs. Most onboarding happened online, with recourse to a manual process if the online process failed. In some cases the CDD was outsourced to PMs. The EMIs’ CDD was adequate when onboarding corporate customers and PMs. Most EMIs were screening for PEPs and sanctioned individuals at onboarding, but the frequency of re-screening was less consistent.

EDD is required for higher risk situations. The MLRs amended the previous scope of a PEP, although only a minority of EMIs onboarded PEPs. PEPs which were onboarded made up a relatively small proportion of the EMIs’ customer bases. EMIs usually conducted EDD when onboarding business customers, and some EMIs did this before establishing the business relationship.

**Policies and procedures**

Most EMIs had revised and updated their policies and procedures to comply with the MLRs. The EMIs took different, but successful, approaches to complying with the changes introduced by the MLRs, including tightening up on CDD.
Training, Communication and awareness
All 13 EMIs had mandatory annual anti-money laundering and sanctions training for staff and new joiners. The training method varied across the EMIs (examples included computer-based training and external consultants). The content of the training also differed, but at one EMI the content was too basic because it focused only on reporting suspicious transactions, whereas it should also have included the changes introduced by the MLRs and an explanation of their impact and significance to the EMI.

Ongoing monitoring
Most EMIs fulfilled their transaction monitoring obligations through automated technical solutions. The FCA noted that sophisticated electronic systems were not required to monitor effectively, but such systems did allow the EMIs to deal effectively with larger volumes of transactions. In larger EMIs, the monitoring was in ‘real-time’ and generated alerts when unusual activity was detected. These alerts were followed up in most cases. Most EMIs carried out periodic reviews of high-risk relationships. Implicit in the review is the FCA’s support of automated monitoring, which allows for greater accuracy and efficiency.

Outsourcing
Five EMIs outsourced marketing and distribution of e-money to PMs. CDD was generally conducted by the PMs, although the legal responsibility remains with the EMI. The extent of the outsourcing to the PMs differed among these EMIs. Outsourcing to PMs was effective when the EMIs displayed a robust governance and oversight of the PMs and conducted effective audits of the PMs. Some EMIs visited PMs on-site regularly, whilst others conducted file reviews or requested management information on the screening process. It was found that the majority of EMIs which did outsource the distribution of e-money and compliance to PMs had “adequate governance and audit measures to manage the risks”.

EMIs approached compliance in different ways, which was supported by the FCA who took a substance over form approach. Going forward, the FCA intends to continue to monitor e-money firms. The full Thematic Review can be accessed here: https://www.fca.org.uk/publications/thematic-reviews/tr18-3-money-laundering-and-terrorist-financing-risks-e-money-sector.

Claudia Barry, Trainee Solicitor, London

A bank was ordered to disclose, to a customer, suspicious activity reports (SARs) that the bank had sent to the National Crime Agency (NCA) at the time of freezing the customer’s bank accounts. The bank’s arguments concerning confidentiality, tipping-off and prejudicing an investigation were unsuccessful. The court’s observations on the interplay between the SARs regime and the law on data protection, defamation and breach of contract will be of interest to all banks.

Suspicious Activity Reports – a reminder

The UK’s substantive money laundering offences and associated defences are contained in the Proceeds of Crime Act 2002 (POCA). Under POCA, entities operating in the regulated sector (essentially, those offering financial services) may seek a defence to a substantive money laundering offence by making a Suspicious Activity Report (a SAR) to the National Crime Agency (NCA) prior to taking any steps in relation to the funds it suspects to constitute the proceeds of crime. When a SAR has been submitted a bank will freeze the suspicious accounts. If it has not received a ‘notice of refusal’ in relation to its proposed steps from the NCA within seven working days it may unfreeze the account. The level of suspicion required to attach criminal liability for money laundering is low – and, in part, is a subjective test.

Bank submits SARs and freezes accounts

The bank froze a joint account belonging to one of its customers, a barrister, for eight days. Nine months later, it went on to freeze seven other accounts held by the same customer – a personal account, another joint account and four business accounts. Upon a request from the customer to access documents relating to the freezing of his accounts, the bank provided limited documentary evidence, and did not disclose copies of the SARs it had made to the NCA.

Customer does not believe bank held genuine suspicion

The customer launched a multi-pronged attack on the bank’s actions, including claims for breach of contract, defamation, breach of the Data Protection Act 1998 (the acts took place prior to the entry into force of the General Data Protection Regulation) and also an application for disclosure of the SARs. Implicit in all these claims was the customer’s belief that the bank did not hold a genuine suspicion that the money in his accounts constituted the proceeds of crime, that his accounts had been unnecessarily frozen and his reputation damaged.

The customer wanted to see the SARs and information held by the bank, which was relevant to its decision to make the SARs and freeze (and unfreeze) his accounts. He sought summary judgment on his claims (summarised below).
<table>
<thead>
<tr>
<th>Customer’s claims</th>
<th>Bank’s defence/application</th>
<th>Court’s ruling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breach of contract: the bank was in breach of contract by failing to follow the accountholder’s instructions and by failing to evidence that it had a genuine suspicion that the account held criminal proceeds.</td>
<td>Express contractual provisions allowed bank to freeze accounts if not to do so would expose it to criminal liability.</td>
<td>Not a matter for summary judgment since it involved questions of fact – the bank must show that it held the relevant suspicion.</td>
</tr>
<tr>
<td>Breach of DPA 1998: the bank (1) had not provided in time (or at all) all personal data in response to the data subject access request and (2) the data provided was not in intelligible form and it included inaccurate information.</td>
<td>The decision to freeze accounts did not concern ‘personal data’. The information sought contained that of other individuals (so it was mixed data) and there was an exemption for the prevention and detection of crime.</td>
<td>The customer’s claim was not a matter for summary judgment. However, the bank’s approach to determining whether information was the customer’s personal data was “clearly flawed” and the customer had a “strong claim” that the bank’s deliberations and decision to submit SARs and freeze and unfreeze accounts was his personal data. Accordingly the bank’s application for strike out/summary dismissal was rejected.</td>
</tr>
<tr>
<td>Defamation: the bank had defamed the customer by suggesting that it had suspicions that his account contained criminal proceeds. Defamatory statements were published in the SARs and in internal bank employee communications concerning the decision to make the SARs and freeze the accounts.</td>
<td>The statements were not defamatory, not published, did not cause harm and in any case were protected by qualified privilege.</td>
<td>Not a matter for summary judgment: statements were capable of being defamatory and they were published. However qualified privilege was likely to apply, subject to malice.</td>
</tr>
<tr>
<td>Inspection: The customer was entitled to see the SARs as they had been referred to in the bank’s defence and counterclaim.</td>
<td>SARs are, in general, confidential, and these SARs were disclosed to the NCA in the strictest confidence. Permitting inspection of the SARs may expose the bank to the offence of tipping-off or prejudicing an investigation. Inspection was not necessary for fair disposal of action.</td>
<td>The SARs in question must be disclosed after 14 days of the court’s order (to enable the NCA to consider its position on making such disclosure). There was no evidence that inspection would trigger tipping-off. There was no evidence that they are required to be kept confidential. The SARs were plainly relevant to the assessment of whether the bank’s employees genuinely held a relevant suspicion.</td>
</tr>
</tbody>
</table>
Impact of decision

This was a summary judgment/strike out application, so is of limited precedent value. The case has settled, so we will not see the issues that arose fully resolved.

We are not expecting this decision to cause a rush by customers to bring claims of this sort against banks:

- The English courts have historically provided banks with considerable protection and discretion relating to SARs due to the fact that banks are merely seeking to help law enforcement and avoid criminal liability. The courts would not want to encourage civil claims of this sort.
- It is hard to imagine a situation where a bank would file a SAR without a genuinely held suspicion (even if that suspicion turns out to be unfounded).
- Many customers would be deterred by the potential cost and the risks of litigation. The claimant in this case was a barrister, who represented himself, so these concerns may have been less of an issue for him.
- The ruling does however provide a reminder that should a bank be faced with a similar claim, it is very unlikely to be able easily and quickly to defeat it (by way of strike out). The ruling makes clear that the question of whether a bank has a genuine suspicion that money in an account was criminal property is a primary fact for the bank to prove at trial.
- Banks may start receiving data subject access requests for personal data relating to SARs. The judge’s view on this summary judgment application was that there was a “strong case” that a bank’s deliberations and decision to submit SARs and freeze accounts constituted personal data, and that the bank had demonstrated “a flawed understanding of the scope of that concept”. Since it was a summary judgment application, the judge felt unable to address whether the exemption relating to the prevention or detection of crime was available stating “[t]here is no evidence before me regarding the likelihood of the provision of further personal data to Mr Lonsdale prejudicing the prevention and detection of crime.” It is difficult to imagine that the rules relating to tipping-off would not prevail since it seems to be a paradigm example of what the crime exemption was aimed at (provided the bank held a genuine suspicion). It is a shame that the judge did not feel able to make this finding even on a summary basis.

Looking ahead

There is a call for reform to the UK’s SARs regime. The OECD has criticised the UK for the low level of corruption enforcement activity from the current regime. A UK Law Commission consultation states that there are on average 2000 SARs filed per day with the NCA, many of ‘low quality’, making it hard for investigation authorities to detect where the real risks are.

The low level test for suspicion for the substantive money laundering offences in the UK has also been criticised in the consultation. “A majority of stakeholders expressed the view that suspicion remains ill-defined, unclear and inconsistently applied by banks and businesses.” This leads to defensive reporting where reports are made more because of concerns regarding a failure to comply with POCA than because of genuine suspicion.

The Law Commission recommends improvements to the SARs regime in particular suggesting that better guidance on ‘suspicion’ would lead to better quality SARs.

Arnondo Chakrabarti and Eve Giles, both Partners, London and Amy Edwards and Jason Rix, both Senior Professional Support Lawyers, London
As previously reported in the Q2 2018 edition of Allen & Overy’s European White Collar Crime Report, the European Fifth Anti-Money Laundering Directive (5MLD) entered into force on 9 July 2018, with an implementation deadline of 10 January 2020 (which may include the UK, depending on the terms of the Brexit transition period) and an implementation date of 10 January 2019 for provisions relating to anonymous safe deposit boxes.

5MLD imposes additional obligations, particularly on those in the finance sector and aims to, among other things, improve enforcement of 4MLD and to ensure tighter controls relating to high-risk third countries.

Among the changes introduced by 5MLD is the requirement to provide wider access to each Member State’s central register of beneficial ownership of corporate entities. Under 5MLD, these registers can now be accessed by the general public without the need for them to show a ‘legitimate interest’.

The table below provides an overview of how some Member States are implementing the requirement to maintain UBO Registers in their national law. Please see the following page for a summary of the implementation status of 4MLD.

<table>
<thead>
<tr>
<th>Country</th>
<th>5MLD and UBO register implementation status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>Legislative work has started on a draft bill implementing the 5MLD. No specific date can however be anticipated as to when the draft bill will be submitted to and passed by the Parliament. The UBO Register went live on 1 October 2018. Belgian companies and other relevant entities have until 31 March 2019 to upload and complete beneficial ownership information on the UBO Register. The Royal Decree of 30 August 2018 on the operating procedures of the UBO Register has implemented both the 4MLD and 5MLD requirements in relation to the completion, functioning of and access to the Register. Members of the public have restricted access to the UBO Register and will have to identify themselves through eID, and may only search the Register using a company’s Crossroads Bank for Enterprises number or company name. Given that companies have until end of March 2019 to update the Register, it seems likely that the Register will be lacking information until this deadline.</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>The implementation of 5MLD is at an early stage in the Czech Republic but it has been flagged that significant changes to the Czech rules which govern UBOs are to be expected. The rules are likely to become more detailed as they seek to implement 5MLD.</td>
</tr>
<tr>
<td>France</td>
<td>5MLD is yet to be fully transposed into French law, although a draft bill is currently being considered by the French Parliament in order to allow the Government to transpose the directive through orders. In response to the implementation of 4MLD, a new decree entered into force on 21 April 2018 which includes provisions on UBOs. This decree specifies what is meant by a ‘beneficial owner’ – this includes whether the owner owns, directly or indirectly, more than 25% of the capital or votes, or if they have control over the company in a way which allows them to determine decisions in general assemblies of the company.</td>
</tr>
<tr>
<td>Country</td>
<td>5MLD and UBO register implementation status</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Germany</td>
<td>5MLD is yet to be implemented in Germany. 4MLD has been effective since 26 June 2017 in Germany and this established the German UBO Register. The requirement under 5MLD that UBO Registers are to be public is still to be satisfied as the current register only grants immediate access to certain authorities and individuals who can show they have a ‘legitimate interest’.</td>
</tr>
<tr>
<td>Hungary</td>
<td>The deadline for the database setup in relation to the implementation of the UBO Register in Hungary is 1 January 2019. Currently, third persons may request data from the central register but this is granted to those with a ‘legitimate interest’ only.</td>
</tr>
<tr>
<td>Italy</td>
<td>The UBO Register has not yet been implemented in Italy despite 4MLD having been implemented by Decree no. 90/2017. Second-level legislation is required to provide details on how companies’ obligations to disclose their UBOs should be carried out in practice, however, the deadline for issuing second-level legislation expired in July 2018. The implementation of the UBO Register could be postponed until after the implementation of 5MLD.</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Two UBO registers are in the process of being created in Luxembourg by two different laws. On the one hand, bill of law no. 7217 pertaining to the register of beneficial owners of companies and similar entities registered with the Luxembourg trade and companies register has been adopted through the Law of 13 January 2019 (the RBE Law). On the other hand, bill of law no. 7216, which was introduced before the Luxembourg Parliament on 6 December 2017 and implemented article 31 of the 4MLD pertaining to the register of trusts, has been divided into two separate bills following the adoption of the 5MLD: the first containing the information to be obtained and retained by trustees (no. 7216A) and the second concerning the register of trusts (no. 7216B). Bill no. 7216A has been adopted through the Law of 10 August 2018 regarding the information to be obtained and retained by trustees. Bill no. 7216B is still undergoing the standard legislative process and there is no visibility on the date on which the final law will be adopted. The transposition of 5MLD has not started yet, except that the law creating the RBE already anticipates a couple of changes required by 5MLD: access to the RBE will be granted to any person and beneficial owners of an entity registered in the RBE have an explicit obligation to provide all relevant information to that entity.</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>5MLD has not yet been implemented in the Netherlands. The UBO Register has also not yet been implemented in the Netherlands. Although first steps for the implementation were taken, the process was put on hold due to the 5MLD coming into force. The deadline for the implementation was then extended to 18 months after the 5MLD went into force, meaning that the UBO Register should be implemented by 30 November 2019. In December 2018, the Dutch Minister of Finance informed the Dutch Parliament that a new draft bill regarding the UBO register is set to be published in March 2019. As of 18 March 2019, no such draft bill was published.</td>
</tr>
<tr>
<td>Poland</td>
<td>The act which implemented 4MLD postponed the implementation of a UBO Register until 13 October 2019 in Poland. The relevant ministry of the Polish Government has confirmed that it has not yet started working on the implementation of the additional requirements of 5MLD.</td>
</tr>
<tr>
<td>Country</td>
<td>5MLD and UBO register implementation status</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Romania</td>
<td>4MLD has not yet been adopted in Romania and the EC has begun infringement procedures in respect of this. The current draft law which would transpose 4MLD into Romanian law does not include provisions which would meet the 5MLD requirements on UBO registers.</td>
</tr>
<tr>
<td>Spain</td>
<td>5MLD has not yet been implemented in Spain although the Spanish Council of Ministers approved Royal Decree 11/2018 in August 2018 on the transposition of a number of directives, which includes the prevention of money laundering. This entered into force on 4 September 2018 and incorporates 4MLD within Spanish law. It requires entities subject to 4MLD to indicate their real owners and to keep a record of this in a marginal note within the relevant Commercial Registry filing.</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Provisions regarding anonymous safe deposit boxes implemented by 10 January 2019. As noted above, Member States are required to transpose the remainder of MLD 5 by 10 January 2020. This will be after the UK has formally left the EU, but within the transitional period currently envisaged in the draft EU Withdrawal Agreement. It is therefore assumed that the UK will implement 5MLD in full.</td>
</tr>
</tbody>
</table>

The table below summarises the status of 4MLD’s implementation as at the end of Q4 2018 in various Members States:

<table>
<thead>
<tr>
<th>Country</th>
<th>4MLD implementation status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>Effective from 16 October 2017. The Belgian legislature has adopted the Act of 18 September 2017 on the prevention of money laundering and the financing of terrorism and on restricting the use of cash (Wet van 18 September 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten; Loi du 18 Septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces).</td>
</tr>
<tr>
<td>France</td>
<td>Order No. 2016-1635 of 1 December 2016 still yet to be ratified by French Parliament, in order to have statutory force. Many provisions of Decree No. 2018-284 dated 18 April 2018 came into force on 1 October 2018.</td>
</tr>
<tr>
<td>Germany</td>
<td>Effective from 26 June 2017. Money Laundering Act (Geldwaschegesetz).</td>
</tr>
<tr>
<td>Country</td>
<td>4MLD implementation status</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>legislative package implementing 4MLD in Luxembourg is composed of:</td>
</tr>
<tr>
<td></td>
<td>– the tax reform law of 23 December 2016, which has led to the insertion of criminal tax offences (<em>fraude fiscale aggravée et escroquerie fiscale</em>) into the list of predicate offences to money laundering;</td>
</tr>
<tr>
<td></td>
<td>– the Luxembourg Law of 13 February 2018: it implements the main provisions of the 4MLD and amends the amended law of 12 November 2004 on the fight against money laundering and financing of terrorism;</td>
</tr>
<tr>
<td></td>
<td>– the Luxembourg Law of 1 August 2018: it implements Directive No. 2016/2258 pursuant to which national tax authorities shall be granted access to the mechanisms, procedures, documents and information referred to in articles 13 and 40 of the 4MLD;</td>
</tr>
<tr>
<td></td>
<td>– the Luxembourg Law of 10 August 2018 which amended the amended Law of 12 November 2004 on the fight against money laundering and the financing of terrorism, in order to ensure compliance with 4MLD (amendments relate to the Financial Intelligence Unit (<em>Cellule de Renseignement Financier CRF</em>));</td>
</tr>
<tr>
<td></td>
<td>– Bill no.7216, which was introduced before the Luxembourg Parliament on 6 December 2017 and implemented article 31 of the 4MLD pertaining to the register of trusts, has been divided into two separate bills following the adoption of the 5MLD: the first containing the information to be obtained and retained by trustees (no.7216A) and the second concerning the register (no.7216B);</td>
</tr>
<tr>
<td></td>
<td>– Bill no. 7216A has been adopted through the Law of 10 August 2018 regarding the information to be obtained and retained by trustees. Bill no.7216B is still undergoing the standard legislative process and there is no visibility on the date on which the final law will be adopted. Following the adoption of 5MLD, the bill is expected to be amended notably so as to extend to any Luxembourg fiducial arrangement; and</td>
</tr>
<tr>
<td></td>
<td>– the Luxembourg law of 13 January 2019 pertaining to the register of beneficial owners (RBE) and implementing the provisions of article 30 of the 4MLD (the RBE Law), published in the Luxembourg official journal on 15 January 2019. The RBE Law will come into force on the first day of the second month following that of its publication in the Luxembourg official gazette (ie on 1 March 2019). Subject entities will then have six months to comply with the provisions of the RBE Law.</td>
</tr>
</tbody>
</table>

The A forthcoming Grand Ducal Regulation will address the technical aspects relating to the RBE Law such as the costs of the registry, the modalities for an electronic registration or the right to access the registry.

This legislative package has been completed by the guidelines issued by the three European Supervisory Authorities (EBA/ESMA/EIOPA) on money laundering and terrorist financing risk factors which were adopted in Luxembourg via CSSF Circular 17/661 entered into force on 26 June 2018.

It is also worth mentioning that a bill of law no. 7356 amending the Luxembourg Criminal Code and providing *inter alia* certain definitions of terrorist financing was introduced before the Luxembourg Parliament on 13 September 2018 and is currently undergoing the standard legislative process. Bill of law no. 7356 implements Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.
<table>
<thead>
<tr>
<th>Country</th>
<th>4MLD implementation status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poland</td>
<td>4MLD was implemented by the new Act on Counteracting Money Laundering and on the Financing of Terrorism dated 1 March 2018 which was published on 12 April 2018. It came into force on 13 July 2018, with the exception of Chapter 6 and Articles 194 and 195 concerning the establishment of a Central Register of Beneficial Owners, which will come into force on 13 October 2019.</td>
</tr>
<tr>
<td>Romania</td>
<td>Not yet implemented. After its adoption, the draft law has been sent back to the Parliament in order to be amended, so that it complies with the Romanian Constitution. This process may take several months. Given that the deadline for implementing the Fourth AML Directive elapsed, it is possible that the Government may issue an emergency ordinance to expedite the process.</td>
</tr>
<tr>
<td>Slovakia</td>
<td>4MLD was implemented in Slovakia via Act No. 52/2018 Coll., which was an amendment to the Slovak Anti-Money Laundering Act. The amendment took effect on 15 March 2018, although certain selected provisions will only come into effect on 1 November 2018.</td>
</tr>
<tr>
<td>Spain</td>
<td>Effective from 4 September 2018. On 30 August, the Spanish Council of Ministers approved Royal Decree 11/2018, 31 August, on the transposition of directives on the protection of pension commitments with workers, prevention of money laundering and requirements for entry and residence of third-country nationals, which incorporates the IV AMLD within Spanish law, and amends Law 10/2010, of April 28, on the prevention of money laundering and the financing of terrorism.</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>Effective from 25 July 2018. Please note that provisions regarding the ultimate beneficial ownership register were implemented in a separate Act.</td>
</tr>
</tbody>
</table>
**French MP and citizens file Cum/ex Files complaint**

In October 2018, the French newspaper *Le Monde* published the results of a media inquiry conducted in collaboration with the European journalist consortium regarding the Cum/ex Files.

*Le Monde* alleged that 'cum/ex' mechanisms were implemented between 2001 and 2007 in EU Member States and caused approximately EUR55 billion in damages. The choice of the Latin term "cum/ex", meaning "with/without", reflects the fact that cum/ex deals involve the buying and selling of shares around a dividend payment date that enable participants to either avoid dividend-withholding taxes or benefit from lower rates.

On the basis of this inquiry, a French MP and a group of French citizens, in their capacity as French tax payers, have filed a complaint with the National Financial Prosecutor, against unidentified persons, for laundering the proceeds of tax evasion and aggravated fraud.

Although the complaint has attracted press attention, the National Financial Prosecutor has not made any official announcements as yet.

Meanwhile, the French Parliament has adopted a new legislative provision in the 2019 Finances Statute ("loi de finances 2019"), the purpose of which is to more efficiently prevent certain illicit 'cum/ex' practices.

**Constitutionality of certain dual tax and criminal sanctions**

A constitutional challenge was brought before the Constitutional Council regarding the fact that the same failure to declare tax can be subject to both administrative tax sanctions and criminal penalties, on the grounds of Articles 1728 and 1741 of the French General Tax Code, in breach of the principles of necessity and proportionality of offences and penalties enshrined in French constitutional law.

The French Constitutional Council held on 23 November 2018 that the dual tax and criminal sanctions provided by the said articles are constitutional, provided that certain conditions are fulfilled, and in particular that where dual sanctions are issued, the total amount of the sanctions must not exceed the maximum amount allowed for one of them (using the highest of the two maximum sanctions), pursuant to the principle of proportionality.

This decision once again highlights that dual sanction regimes are not without limits under French law.

**Leading Swiss bank convicted by the Paris Criminal Court in the biggest alleged money laundering of tax evasion proceeds’ case in French history**

In October and November 2018, a leading Swiss bank appeared for trial before the Paris Criminal Court, alongside its French subsidiary and six executives, on the grounds of laundering the proceeds of tax evasion and illicit solicitation, in what is by far the biggest white-collar crime case in French history.

After seven years of investigations, a EUR1.1bn bail, and aborted settlement negotiations following the enactment of the Sapin II law, the Swiss bank raised several constitutional and nullification arguments before the Court, before defending itself on the merits of the case. While few individuals or corporates have been convicted for illicit solicitation in France, the Paris Criminal Court has convicted several foreign financial institutions on the grounds of money laundering over the past few years, using an extensive interpretation of its jurisdiction and the theory that certain professionals knowingly "turned a blind eye" to their clients' activities.

The French State requested EUR1.6bn in damages and the Public Prosecutors requested an unprecedented EUR3.7bn fine against the Swiss bank.

On 20 February 2019, the Paris Criminal Court issued an unprecedented decision in which it found the Swiss bank guilty of laundering the proceeds of tax evasion and illicit solicitation and sentenced it to an exceptionally severe EUR3.7 billion fine. Its French subsidiary was found guilty of aiding and abetting the said two offences and sentenced to a EUR15 million fine. The Swiss bank was also ordered to pay, jointly and severally with its French subsidiary and three executives (the remaining two executives having been found not guilty of money laundering), EUR800 million in damages to the French State, which had registered as a victim. The Swiss bank immediately filed an appeal against this first instance decision, which could mark the start of a new era for the prosecution of laundering the proceeds of tax evasion in France.
Transactions with ADRs under review by German authorities
The Cologne prosecutor René Seppi has indicated that potential transaction anomalies were under review in respect of “American Depositary Receipts” (ADRs). ADRs are U.S. securities that represent foreign shares of a foreign company. U.S. depository banks are accused of having issued ADRs in circumstances where their customers may have obtained potentially unjustified tax refunds outside the U.S., including in Germany.

As a precautionary measure, the German Ministry of Finance has suspended a digitised reimbursement procedure (Datenträgerverfahren) with regard to ADRs. This procedure was intended to simplify tax refunds but is now being suspected by the authorities as a possible channel for potential misuse.
**Market offences**

**SPAIN**

**Proceedings against directors for accounting misrepresentations**

On 28 June 2011, Spanish bank, Bankia was floated by means of a Public Share Subscription and Trading Admission Offer. To this end, the Spanish National Stock Market Commission was provided with a set of accounting information in a Prospectus that purported to reflect Bankia’s good financial situation. However, weeks later it was discovered that apparently the financial situation compiled in the Prospectus was inaccurate due to the existence of material accounting adjustments not properly reflected in the financial statements (e.g. insufficient level of provisions arising from non-performing loans, as well as, the amount of deferred tax assets recognised). In response, criminal proceedings were initiated against Bankia and its directors.

The trial started on 26 November 2018 before the National Court, and no judgment has yet been handed down. However, the Public Prosecutor’s Office has announced that it could extend its indictment to the crime of accounting misrepresentation (until now, the Public Prosecutor’s Office has only alleged fraud in the financial information contained in the Prospectus).

Accounting misrepresentation entails the falsification, by the directors (de facto or de jure) of a company, of its annual accounts or other documents that reflect the legal or economic situation of the entity, in such a way that may cause economic damage to the entity, to one of its partners, or to a third party.

Although the law provides that only de jure or de facto directors may perpetrate the crime, the auditors, when carrying out the external accounting audit, may also incur criminal liability as cooperators or accomplices. Criminal responsibility is personal and, therefore, only those members of the Board of Directors who voted individually in favour of the accounts (and whose actions satisfy the other elements of the offence) will be held criminally liable.

This represents an expansion of the scope of liability for accounting misrepresentations to the managers; even if a company is provided with an external audit report, approved by its audit committee, board members can still be held liable for their approval in circumstances where they should have monitored the situation more closely (“in vigilando”).

**GERMANY**

**Trading Bitcoin not subject to authorisation**

In a decision handed down on 25 September 2018, the Kammergericht Berlin (case number: 161 Ss 28/18) held that Bitcoin is neither a unit of account, nor a financial instrument, leaving the cryptocurrency unclassified under the German Banking Act (Kreditwesengesetz, KWG).

The case concerned the careless operation of unauthorised bank transactions and saw the Kammergericht reprimand the Financial Supervisory Authority BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) for classifying Bitcoin as a unit of account under the KWG in a published notice.

In the opinion of the Kammergericht, BaFin had exceeded its area of responsibility by shaping the law governing bitcoin. This, it said, had impact on the criminal law given that in Germany it is a criminal offence to trade instruments classified under the KWG without a licence.

In a similar case in 2014, the Berlin Court of Appeal also criticized a BaFin’s notice on investment brokerage. In this note, the BaFin regarded the brokerage of asset management contracts as securities service subject to licensing. Only when the European Court of Justice ruled to the contrary in 2017 BaFin did concede and stopped investigating cases of asset management contract brokerage. According to newspapers, it remains to be seen whether BaFin will use the opportunity afforded by these two decisions to change its administrative practice.
The FCA’s revised guidance on financial crime systems and controls came into force on 13 December 2018. It is aimed at enhancing firms’ understanding of the FCA’s expectations of their financial crime systems and controls and provides practical observations of good and poor market practice.

**New chapter: Insider dealing and market manipulation**

The most significant amendment concerns firms’ obligations under SYSC 6.1.1R (compliance relating to financial crime). A new chapter 8 clarifies that the FCA considers insider dealing and market manipulation (under the Criminal Justice Act 1993 and the Financial Services Act 2012) to fall within the term “financial crime”. The new chapter does not provide guidance for the equivalent civil offences under the Market Abuse Regulation (MAR), as the responsibility for providing such guidance rests, presently at least, with ESMA. However the FCA recognises that firms might not distinguish between the criminal and civil regimes when implementing their controls relating to insider trading and market manipulation and may find it simpler to consider its guidance as applicable to both the criminal and civil regimes.

**The guidance – an overview**

The chapter is split into four key themes with the FCA’s expectations, self-assessment questions for the firm, and examples of good and poor practice set out for each. Throughout the guidance the connection between money laundering risks and insider dealing and market manipulation is emphasised as such activities often lead to the generation and transfer of proceeds of criminal activities. The FCA highlights the importance of firms having frameworks for such offences that interact with each other in a clear and efficient manner, for example a self-assessment question for a firm is: “How does the firm’s MLRO interact with the individual/departments responsible for order and trade surveillance/monitoring?”

**Governance**

The FCA expects senior management to take responsibility for firms’ measures in relation to insider dealing and market manipulation, including being aware of and managing the potential conflict of interest between revenue generation and the risk the firm is exposed to in the furthering of financial crime. Senior management is expected to set the ‘tone from the top’ in dealing with insider dealing and market manipulation, and to ensure its employees have the appropriate training to identify such activities. Senior management should also interact regularly with the MLRO and should not consider the firm’s regulatory obligations to be fulfilled solely by the firm filing Suspicious Transaction and Order Reports (under MAR) and/or Suspicious Activity Reports (under the Proceeds of Crime Act 2002 (POCA)). Senior managers should ensure that the individuals responsible for overseeing a firm’s monitoring of potential insider dealing and market manipulation activity will share relevant information and regularly interact with the firm’s MLRO.

**Risk assessment**

Firms should regularly assess and review the risk of facilitating insider dealing and market manipulation against all its client types and asset classes, including risks posed by the actions of their own employees. For example, firms should consider if employees are able to use discretionary accounts to commit offences. Firms should ensure persons of sufficient expertise and seniority carry out risk assessments, and that the insider dealing and market manipulation risk framework is aligned with the firm’s AML risk framework.

**Policies and procedures**

Firms’ policies and procedures should be designed to counter the risks identified in their risk assessments. These policies and procedures should cover the lifecycle of a transaction from countering the risks of insider dealing and market manipulation pre-trade, to mitigating future risk where suspicious trading, by a client or employee, has already occurred. Firms should ensure that front office staff are able to identify potentially suspicious trading. Where an order is identified as being potentially suspicious, a firm should refuse to execute the trade where possible. Respondents during the FCA’s consultation process raised the concern that refusal to execute trades or terminating a client relationship altogether could ‘tip off’ the client and expose the firm to other potential offences eg the offence of tipping off under s333A POCA. The FCA has clarified it does not
consider refusing to execute potentially suspicious trades to constitute ‘tipping off’ but firms may want to record the rationale, decision making and communications for any actions taken against clients to show clearly the intention of the firm is not to tip off the client.

**Ongoing monitoring**

The FCA suggests firms may be able to use the results of its order and transaction monitoring obligations under MAR for the purpose of countering insider dealing and market manipulation. These monitoring activities may include surveillance of a client’s usual trading behaviour via targeted monitoring of voice and electronic communications, and initial onboarding checks. Where a client is placing orders on behalf of its underlying clients, the firm may try to gain further information by engaging with the client to establish whether they maintain trades to constitute ‘tipping off’ but firms may want to appropriate systems and controls for countering the risk of being used to further financial crime.

However, firms should recognise the scope of the criminal regime is broader than that under MAR in terms of the markets and instruments to which it applies. As a result, firms should assess whether it would be appropriate for them to rely solely on such arrangements.

**Practical impact**

The new information set out in the Guide constitutes FCA guidance, not rules. However, the FCA will take into account whether firms have complied with the guidance when it is determining whether they have complied with the FCA’s rules, e.g. SYSC 6.1.1R and the FCA’s Principles for Businesses. As a result, it is important that firms are aware of this new guidance and assess their current systems and controls against it in order to identify any gaps.

*Nicole Choong, Trainee Solicitor, London*
Czech Republic

Criminal proceedings against doctors and representatives of pharmaceutical companies continue

The State Prosecutor’s Office accused nine physicians of accepting bribes for the illegal promotion of specific medicines. The bribes were allegedly offered by 16 managers, employees and other representatives of two pharmaceutical companies – ICHM Czech s.r.o. (formerly Interchemia Praha, spol. s.r.o.) and GNR Czech s.r.o. (formerly GENERICON s.r.o.) – both of which have already been dissolved. According to the State Prosecutor’s Office, the representatives participated in an organised criminal group focused on the illegal support of generic medicines produced or distributed by the two pharmaceutical companies. The representatives were also included in the accusation which was filed in court on 28 August 2018.

Depending on the amount of accepted bribes (ranging from approx. EUR15,000 to approx. EUR100,000), the doctors can be sentenced for up to ten years’ imprisonment. The representatives are facing similar prison sentences.

European Commission investigates Czech Prime Minister’s interest in AGROFERT

According to the European Commission, the Czech Prime Minister is operating under a conflict of interest which makes independent performance of his position impossible. The alleged conflict of interest concerns the Prime Minister’s interest in AGROFERT, an agricultural holding conglomerate, which regularly receives significant subsidies from EU funds. Until February 2017, the Prime Minister was the sole shareholder of AGROFERT, when he then transferred his holding to various trusts. By virtue of the control he is able to influence over the trustees, the European Commission claims that the Prime Minister continues to indirectly control AGROFERT. The current European Commission investigation follows a previous investigation conducted by the European Anti-Fraud Office (commonly known as OLAF), also into the abuse of EU funding received by AGROFERT.

As a result of the investigations, the Czech Republic may be required to return a minimum of EUR82m to Brussels from its own state budget. Since the conflict of interest has likely existed since 2014 however, the sum to be returned could be much higher.
Major oil and gas company suspected of corrupting foreign public officials appeared for trial at the Paris Criminal Court

In October 2018, a major oil and gas company appeared for trial before the Paris Criminal Court on the grounds of corruption of foreign public officials.

The company was suspected of paying around USD30m in commissions to foreign public officials in order to obtain contracts in Iran.

After already reaching a USD398m settlement in the U.S. for the same facts back in 2013, the company argued that it could not be judged twice for the same facts, pursuant to the ne bis in idem principle.

The success of the argument seemed unlikely, in light of the French Supreme Court’s decision in the Oil-for-Food case in March 2018, where the arguments raised by another major oil company on the basis of the ne bis in idem principle were rejected by the Court.

On 21 December 2018, the Paris Criminal Court handed down its decision, finding the company guilty of corruption of foreign public officials and imposing a fine of EUR500,000.

Ill-gotten gains: French NGO Sherpa files a new complaint against the Djiboutian president and his entourage

In October 2018, the French NGO Sherpa filed a new complaint, alongside the European collective of Djiboutian diaspora, against the Djiboutian president and his entourage, on the grounds of misuse of corporate assets, misuse of public funds, misuse of trust and corruption of foreign public officials.

This complaint could constitute a new saga in the “bien mal acquis” affair, involving the funds used by African Heads of State and their entourages to buy luxurious goods and properties in France, whereby the Vice-President of Equatorial Guinea, Teodorin Obiang, was notably convicted to a three-year suspended imprisonment penalty and a EUR30m fine in 2017.

The complaint focuses on the circumstances in which the Djiboutian President’s family (particularly his wife and son-in-law) bought luxury properties in prestigious areas in Paris.

According to the press, a preliminary investigation has been opened and entrusted to the complex financial crime police force.

Former French President’s campaign director placed under formal investigation for passive corruption

In the context of the criminal investigation targeting the alleged financing of a former French President’s election campaign by the Gaddafi government in 2007, the investigating judges have placed the former French President’s campaign director under formal investigation on the grounds of passive corruption, receiving misused public funds and aiding and abetting the illegal financing of an election campaign.

In particular, the investigators pinpoint the immoderate use of cash by the former French President’s campaign director, highlighting that he had only withdrawn EUR800 from his bank accounts over nearly ten years, from 2003 to 2012.

European public official convicted for active corruption by the Paris Criminal Court

In October 2018, a European public official was convicted by the Paris Criminal Court on the grounds of active corruption, and sentenced to a 15-month imprisonment penalty (entirely suspended) and a EUR150,000 fine, for having provided information to two company directors involved in public procurement, in exchange for wire transfers to his wife.

The defendant has been banned from being a European public official for five years. Along with the two company directors, he has also been jointly and severally ordered to pay the European Commission, which registered as a victim in the case, EUR100,000 in damages on the grounds of moral harm.
GERMANY

**Second attempt to commence proceedings against 2006 World Cup Officials**

In October 2018, the Frankfurt Regional Court rejected the opening of criminal law proceedings against former football officials linked to the 2006 World Cup affair. The Public Prosecutor’s Office had been investigating a serious case of suspected tax evasion for more than two and a half years (since October 2015) and had submitted a 144-page indictment in May 2018. However, the Regional Court did not find sufficient evidence for the tax evasion. The Public Prosecutor’s Office in Frankfurt has lodged an appeal against the decision of the Regional Court. As a next step, the Frankfurt Higher Regional Court must deal with the question of whether there will be criminal law proceedings.

POLAND

**Former Chairmen of the Polish Financial Supervision Authority detained**

Two former chairmen of the main Polish financial regulator are suspects in cases concerning corruption proposals and the improper supervision of financial entities.

In November 2018, the Polish press disclosed a taped conversation between the then-Chairman of the Financial Supervision Authority (the PFSA) and billionaire Leszek Czarnecki, who owns Getin Noble Bank and Idea Bank (the 9th and 11th largest Polish banks based on balance sheet assets). During the conversation the then-Chairman allegedly proposed that Czarnecki should hire and pay a designated lawyer PLN40m (almost EUR10m) in exchange for the Chairman’s support in what he described as a planned government-backed takeover of Czarnecki’s banks. Once Leszek Czarnecki revealed this to the press, the Chairman of the PFSA immediately resigned and was subsequently arrested. A few days later, the Polish Public Prosecutor accused the previous Chairman of the PFSA, Andrzej Jakubiak, and six other high-level officials, including the PFSA’s deputy Chairman, Wojciech Kwaśniak, of negligence from 2011 to 2016 in the credit union SKOK Wołomin case. The credit union went bankrupt in 2015 and the losses incurred by the clients had to be covered by the Bank Guarantee Fund. Both cases sent shockwaves through the financial markets and seem to have eroded at least part of the good reputation that the PFSA and other constituencies of the Polish financial system have earned in the last couple of years.
European Commission reports on progress towards Romanian commitments on judicial reform and the fight against corruption

On 1 January 2007 (when Romania joined the European Union), the EU Commission established the Cooperation and Verification Mechanism (CVM) to assess progress against the commitments made by Romania in the areas of judicial reform and the fight against corruption. The latest report on the fulfilment by Romania of such commitments was published on 13 November 2018. The report notes that while Romania has taken some steps to implement the final 12 recommendations issued by the Commission in January 2017, recent developments have reversed the course of progress and called into question the positive assessment made back in January 2017. To remedy the situation the following measures, among others, were recommended:

- **Justice laws**: to suspend immediately the implementation of the Justice laws and to revise such laws fully taking into account the recommendations under the CVM;
- **Judicial appointments/dismissals**: to suspend immediately all ongoing appointments and dismissal procedures for senior prosecutors and to relaunch a process to appoint a chief prosecutor of the National Anti-Corruption Directorate with proven experience in the prosecution of corruption crimes and with a clear mandate to conduct professional, independent and non-partisan investigations of corruption; and
- **Criminal Codes**: to freeze the entry into force of the changes to the Criminal Code and Criminal Procedure Code and to reopen the revision of the Criminal Code and Criminal Procedure Code fully taking into account the need for compatibility with EU law and international anti-corruption instruments, as well as the recommendations under the CVM and the Venice Commission opinion.

**UK**

Nine individuals convicted in FH Bertling SFO bribery cases

Nine individuals, including a former Managing Director and CFO, were convicted in January 2019 following the SFO’s long-running investigation into FH Bertling, the UK subsidiary of the FH Bertling Group, a shipping and logistics company based in Germany. The individuals and FH Bertling Ltd were charged with various counts of conspiracy to make corrupt payments, contrary to section 1 of the Prevention of Corruption Act 1906 (PCA). Two individuals were also charged with conspiracy to make or accept corrupt payments, contrary to section 1 of the PCA and section 1 of the Criminal Law Act 1977.

The SFO began investigating FH Bertling and several of its senior employees in September 2014, following allegations that FH Bertling had paid bribes to secure a GBP16m freight forwarding contract with another company, ConocoPhillips, for an oil exploration project in the North Sea. Three of the individuals charged in relation to the oil exploration project were acquitted of their charges.

The SFO also investigated FH Bertling for corrupt payments made to an agent of Sonangol, the Angolan state oil company, in order to further FH Bertling’s operations in Angola and secure a contract worth approximately USD20m. The corruption took place between July 2005 and December 2006.

SFO Afren convictions and sentencing

The former CEO and COO of Afren plc (Afren), which is headquartered in the UK, were found guilty of fraud and money laundering offences in October 2018. Afren was an international oil exploration and production company which entered administration in 2015.

The executives were found guilty of fraud for recommending a transaction with Oriental Energy Resources (OER) to the Afren board in 2013, which was worth USD300m, whilst failing to disclose that they would personally benefit from a side agreement with OER under which they would receive USD45m of the payments made by Afren to OER. The payments made by Afren in relation to the transaction were made to a shell company that was controlled by the two executives. They used the money to purchase luxury villas and also paid sums to a small group of OER and Afren employees. The SFO investigation began following a self-report by Afren after an internal investigation into potential breaches of the FCA’s Listing Rules resulted in the discovery of the fraud.

The executives were both found guilty of one count of fraud and two counts of money laundering, contrary to sections 1 and 4 of the Fraud Act 2006 and sections 328 and 329 of POCA respectively, and sentenced to a total of 30 years in prison. They have also been disqualified from being company directors for 14 years for failing to disclose personal interests in a number of high-value transactions, including the transaction with OER.
Although the Netherlands is generally considered low risk when it comes to bribery and corruption, the Dutch Public Prosecution Service (DPPS) has been involved in settling several of the most high-profile cases involving global corporations of the last years. By way of example, the DPPS settled a bribery investigation with SBM Offshore in 2014 for USD240m and participated in the settlements with Vimpelcom (USD795m, of which USD397.5m was for the DPPS) and Telia Company (USD965m, of which USD274m for the DPPS). This settlement practice has increasingly been criticised, and in November 2018, this criticism culminated in a proposal by the Dutch Parliament to order the government to introduce a judicial review mechanism for high-profile settlements.

Settlements
The high-profile settlements mentioned above were reached using a so-called ‘transaction’, whereby the DPPS offers the suspect one or more conditions (such as the payment of a monetary amount) to prevent prosecution. In essence, this is a contract between the DPPS and the suspect and there is a relatively high degree of freedom in drafting the relevant contractual terms. However, for settlements exceeding EUR50,000, the DPPS must follow a specific procedure which requires approvals from the executive board of the DPPS and from the Minister of Justice and Security.

Criticism on settlements
Although settlements of high-profile criminal investigations have always resulted in criticism in the media, this criticism has increased markedly over the last years. This criticism has come from various groups, and has concentrated on (i) the perception of backroom politics and the lack of transparency on the conduct being settled due to the absence of any public hearing, (ii) the lack of development of relevant case law, (iii) the perceived class justice of the high-profile settlement practice and (iv) the risk that the DPPS will abuse its power in cases where the suspect has a significant interest in settling a case quickly. In response to some of these criticisms, the DPPS has changed its practice over the last years, notably increasing transparency through the publication of an (increasingly elaborate) statement of facts and, recently, the publication of the signed settlement agreement.

Judicial oversight
In 2018, the criticism on high-profile settlements not only increased in tone and intensity, but was also echoed in formal judicial documents. Most notably, the Dutch Council for the Judiciary (a representative body of courts in the Netherlands) voiced similar concerns publicly and through a formal advice to change the Dutch Code of Criminal Procedure by introducing judicial oversight of high-profile criminal settlements. In November 2018, this resulted in the Dutch Parliament ordering the government to introduce a judicial review mechanism for high-profile settlements. The Dutch Minister of Justice and Safety stated that he will, in consultation with the DPPS and the judiciary, draw up such a mechanism. It is at this time unclear how and when judicial oversight to high-profile criminal settlements will be introduced, with some suggesting to adopt a system similar to the UK’s DPA procedure.

Although much of the criticism on the current high-profile settlements assumes that companies entering into such settlement are ‘getting a sweet deal,’ that does not mean that the introduction of a judicial review mechanism is necessarily detrimental for the settling company. As noted above, some criticism focuses on the risk that the DPPS abuses its powerful position in settlement negotiations. Depending on the way that judicial oversight would be implemented, companies might be better protected against pressure to settle crimes that cannot be proven beyond reasonable doubt. In the meantime, the one thing that is clear, is that the procedure through which high-profile corruption cases will be resolved, is likely to change significantly in the coming period. This is particularly relevant for companies currently facing investigations as this creates even more uncertainty with respect to the expected consequences of such investigations.

Neyah van der Aa, Senior Associate and Jurian van Galen, Associate, Amsterdam
Detailed guidance issued on the reasonable prevention procedures entities should have in place to protect them from criminal liability

In December 2016, a so-called large amendment to the act on criminal liability of legal entities and proceedings against them came into force. The amendment softened the original concept of strict liability of a legal entity for acts committed by the legal entity’s personnel such as members of its statutory body, persons acting on behalf of the legal entity under a power of attorney, persons carrying out management or supervisory activities, employees, or persons exercising a decisive influence on the management of the legal entity.

Under the amendment, the legal entity is able to discharge itself from liability for the acts of these persons if it has made all efforts that could reasonably be expected of it to prevent the commission of a crime.

Until very recently, there was uncertainty as to what specific steps a legal entity should take to protect itself from criminal liability. In August 2018, the Supreme State Prosecutor’s Office issued detailed guidance on this issue. The guidance requires legal entities to implement an effective compliance management system in the form of general principles, rules, recommendations and procedures to prevent crimes from being committed by the legal entity’s personnel. The compliance system should be proportionate to the size of the legal entity, its international reach, risk profile and the sector in which it operates.

Each compliance system should consist of three pillars - prevention, detection and reaction.

The guidance requires each legal entity to:
- conduct a risk analysis;
- introduce and implement a code of ethics or a set of compliance rules and principles reflecting the findings of the risk analysis;
- perform an in-depth due diligence on its business partners;
- introduce regular training for personnel; and
- conduct due diligence and follow-up regular screening of employees.

Tone from the top is crucial for the prevention phase of the compliance system. The detection pillar should comprise measures that will enable identification of violations, such as whistleblowing and internal investigation procedures followed by corrective measures (including labour law implications), and an immediate revision of the compliance system, if necessary. Continuous monitoring of implementation throughout the entire organisation and reporting identified misconduct to law enforcement authorities should form an integral part of the compliance system’s reaction measures.

Even though the guidance is primarily addressed to state prosecutors who assess the criminal liability of legal entities, it provides useful guidance for legal entities. Regulation of corporate criminal liability in the Czech Republic has thus moved one step closer to creating legal certainty and meeting international standards.
**UK**

**Successful conclusion to the UK’s first Deferred Prosecution Agreement**

Following the suspension of an indictment alleging failure to prevent bribery contrary to section 7 of the Bribery Act 2010, the UK’s first Deferred Prosecution Agreement (DPA) was entered into between the Serious Fraud Office (the SFO) and Standard Bank PLC (Standard Bank) in 2016. On 30 November 2018, the SFO announced that Standard Bank has now fully complied with the terms of this DPA.

The DPA related to a payment of USD6m by a former Tanzanian subsidiary of Standard Bank to a local partner in Tanzania. The SFO alleged that the payment intended to induce members of the Government of Tanzania to show preference to Standard Bank’s proposal for private placement of USD600m by the Government.

**UK expands availability of deferred prosecution agreements**

A DPA can now be entered into in respect of offences under ss 89, 90 and 91 of the Financial Services Act 2012 (FSA).

The Crime and Courts Act 2013 (the Act) (Deferred Prosecution Agreements) (Amendment of Specified Offences) Order 2018 (the Order) came into force on 8 October 2018. The Order removes the section 397 offence (making misleading statements and practices) of the Financial Services and Markets Act 2000 (FSMA) from the Part 2 list, following its repeal by the FSA. Conduct that fell within the repealed offence is now covered by three new offences in the FSA that fall within the scope of a DPA, at sections 89 (misleading statements), 90 (misleading impressions) and 91 (misleading statements etc. in relation to benchmarks).

In the UK’s inaugural DPA, Standard Bank was ordered to pay financial orders of USD25.2m and compensation of USD7m to the Government of Tanzania. Standard Bank also agreed to pay GBP330,000 to the SFO for reasonable costs incurred in relation to the case. In accordance with the DPA, Standard Bank also commissioned an external consultant to report on its anti-bribery and corruption procedures. These reports were regularly issued to the SFO during the life of the DPA.

Interestingly though, at present, the FCA which in practice is the lead prosecutor for offences under the FSA is not a designated prosecutor for the purposes of DPAs.

**Europol signs MoU with Diebold Nixdorf**

Europol joins forces with Diebold Nixdorf, a multinational technology company and provider of self-service transaction systems such as ATMs and point-of-sale terminals, as the pair signs a Memorandum of Understanding (MoU) in The Hague. Signed on 16 November 2018, the MoU will see its signatories share major cyber threat intelligence, knowledge related to organised crime activity and exchange expertise with the view to target online crime and strengthen cybersecurity for EU citizens, businesses and governments.
With a stated aim to “make the world even more inhospitable for those who would lie, cheat, steal and bribe to line their pockets” and secured funding of GBP53m for the next three years, the new director of the UK’s Serious Fraud Office (SFO), Lisa Osofsky, is ambitious for the future of the agency.

In a series of speeches and interviews, key figures from the SFO have revealed the organisation’s priorities and hinted at its future strategic direction. With a focus on collaboration, transparency and efficiency, the SFO hopes to make the UK a high-risk place for the world’s most sophisticated criminals to operate.

**International and domestic collaboration**

The key message from the SFO in recent months has been the importance of collaborating with fellow law enforcement agencies, both domestically and abroad. Osofsky believes that such collaboration is vital in order to bring strong and effective cases.

Given the increasingly international nature of white collar crime, it is perhaps unsurprising to see growing cooperation between prosecutors and regulators around the world. The SFO has found that it is often easier and quicker to obtain evidence from overseas where another jurisdiction is investigating similar conduct.

Such collaboration led to the joint settlement between Rolls Royce and the UK, U.S. and Brazil.

Understanding the differences and similarities between jurisdictions is key to such efforts – and this has been aided by secondments. A prosecutor from the U.S. Department of Justice has been recently seconded to the SFO for a year, and two prosecutors from the Singapore Attorney General’s office joined the agency in January 2019.

Osofsky has also emphasised the role that collaboration with other domestic agencies will continue to play in the SFO’s work. The agency has affirmed its close links to the FCA, NCA and the police, and has sent secondees to the UK’s newly formed National Economic Crime Centre.

**Corporate cooperation and integrity**

Both Osofsky and Hannah von Dadelszen, the SFO’s Head of Fraud, have underlined the importance of corporate cooperation in their investigations. They have stressed that corporate leaders who, in their view, obstruct the progress of cases, mislead the SFO or cause unnecessary delays may not benefit from cooperation credit.

The level of cooperation the SFO now expects from corporations is high. They will be expected to make documents, financial records and witnesses available promptly; to point the SFO to the most relevant evidence, rather than ‘document dump’; to make such evidence available in a legal and useful way; and to avoid creating proof issues or procedural barriers. According to the SFO, this level of ethical corporate behaviour is required in order to qualify for a Deferred Prosecution Agreement (DPA), and Osofsky has stressed that DPAs will not be available to those organisations who fail to follow these guidelines.

Furthermore, the SFO maintains that this ethical corporate behaviour should begin even before an investigation is launched. The SFO has therefore placed a renewed emphasis on ongoing corporate compliance and integrity, which must be more than mere ‘window dressing’. Favourable dispositions will not be available to corporations unless their compliance systems are functioning and thorough.

In addition, Osofsky has brought to the SFO a greater emphasis on individuals being awarded immunity from prosecution where they cooperate and provide evidence against others.

**Investigating at pace**

In a speech in late 2018, Matthew Wagstaff, the SFO’s Joint Head of Bribery and Corruption, acknowledged that much of the criticism directed at the agency is brought about by frustration at the length of time it takes them to resolve cases.
The advance of technology has fundamentally changed the investigative process, according to Osofsky. Whereas previously law enforcement agencies suffered from a lack of information, now the problem lies in finding “evidential needles in huge digital haystacks”. The large volume of data the SFO is required to sift through, combined with the increasingly international nature of the work, means that investigating and charging at pace will always be difficult.

However, Osofsky has made a clear commitment to get cases moving quickly, especially at the investigation stage. She told the UK parliament’s Justice Committee that she aims to bring a “more proactive, nimble approach” to the SFO in order to give the public greater confidence in the agency. As a starting point, this will entail being strategic about what lines of enquiry to pursue, presenting cases in a simple and jury friendly manner, and dealing swiftly with delaying tactics.

**Working with technology and legislative tools**

Another key way in which the SFO hopes to increase the pace of investigations is through the use of technology and carefully chosen legislative tools.

Although advances in technology may have contributed to the vast amount of data thrown up by each case, the SFO considers that technology will also provide the tools with which to tackle the problem. For example, Osofsky has indicated that technological developments can help the SFO to access the varied ways in which criminals now communicate and lead them more quickly to exculpatory documents. Indeed, the SFO has invested in an AI-powered ‘Robo-Lawyer’ which can rapidly review documents for legal professional privilege before they are handed over to the case team.

Using the correct legislative tools is also important for the SFO to be effective. There have been calls from the agency to increase individual director liability for corporate failures, to make up for the difficulty they have faced in prosecuting corporates. The much-quoted ‘failure to prevent economic crime’ offence would likely be modelled on section 7 of the UK’s Bribery Act – the ‘failure to prevent bribery’ offence – and would no doubt increase the SFO’s workload considerably were it to be made law. The government’s response to its call for evidence is expected imminently.

*David Siesage, Trainee Solicitor, London*
The U.S., EU and the UK authorities have taken steps to make it much easier and quicker for criminal investigators to access electronic data stored abroad. Digital evidence is required in many cases – around 85% of EU criminal investigations, according to the EU Commission, and, in two-thirds of those cases, the evidence is held by an overseas service provider, causing the rate of EU investigators requesting data from those providers to raise by 84% from 2013 – 2018.

Large technology companies are already being targeted by investigators to access their data in order to assist with criminal investigations involving third parties. There has recently been a huge growth in mutual legal assistance requests to access online records (such as subscriber details, email content, metadata and social media) from these companies, but the process is very slow. The new proposals are aimed at making it much quicker for investigators to access data held abroad.

The U.S. implemented the CLOUD Act (Clarifying Lawful Overseas Use of Data) in March 2018. The CLOUD Act allows the U.S. government to enter into bilateral executive agreements with other countries to expedite cross-border requests by one government for data stored in the other country. There are already plans afoot for such an agreement between the U.S. and the EU – the EU Commission announced on 5 February 2019 its intention to negotiate an EU-wide agreement with the U.S. that would require service providers on both sides of the Atlantic to supply requested electronic data in criminal cases within 10 days.

In the UK the Crime (Overseas Production Orders) Act 2019, enacted on 12 February 2019 will allow UK law enforcement agencies to apply to an English court for an overseas production order to obtain electronic data directly from service providers based outside the UK, for the purposes of criminal investigations and prosecutions for serious crime, without the involvement of the authorities in the country where the evidence is stored. There must first be a “designated international co-operation arrangement” in place between the UK and the jurisdiction from where the data is sought. For this reason, the UK government is working hard to agree a U.S./UK Data Access Agreement as soon as possible. Note that although the existing UK Investigatory Powers Act 2016 allows for the acquisition of data held overseas for investigation purposes, it does not apply to the use of such data on an evidential basis.

On inter-EU Member State collaboration, a regulation on European Production and Preservation Orders for electronic evidence in criminal matters is being passed at EU level which will allow Member State authorities to obtain data directly from companies in other Member States. The UK has decided not to opt into this.¹

Amy Edwards, Senior Professional Support Lawyer, London

---

¹ Hansard HC Deb, 22 October 2018, cWS
The UK’s Financial Conduct Authority (the FCA) has published the first set of aggregated results from its new annual survey of over 2,000 firms on financial crime. Firms within the UK and across Europe may find the insights helpful when considering the adequacy of their identification of high-risk customers and management of suspicious activity reporting by comparing their own management information against industry-wide trends and averages reported in the survey. It also offers a window into market participants’ views on forward-looking trends into 2019 for expected financial crime risks (both by activity type and by country) and action being taken by law enforcement to combat these risks.

Financial crime remains high on the FCA’s agenda. In addition to enforcement action and rhetoric, the FCA’s understanding of the scope of financial crime threats in the UK has been bolstered by the responses to the financial crime return (termed the “REP-CRIM” by the FCA). Since 31 December 2016, the FCA has required over 2,000 firms subject to the UK Money Laundering Regulations, including all UK banks and building societies, to submit an annual financial crime data return.

In November 2018, the FCA published its first industry-wide report analysing the aggregated financial crime threats and trends identified in the survey responses. The results provide a useful overview across the surveyed firms of: (i) the number and nature of high-risk customer relationships maintained in the UK; (ii) ongoing work within those firms to combat financial crime; and (iii) industry perceptions on specific fraud and country risks.

Statistics on the overall number of high-risk customers in the UK

The respondent firms had a customer base consisting of approximately 549m relationships, of which only 120,000 involved ‘politically exposed persons’ (PEPs) (an overall share of 0.02% of total customers) and 1.6m other ‘high-risk customers’ (an overall share of 0.29% of total customers).

It is possible that the FCA could use this industry-wide data to target firms for additional supervision in terms of AML controls. For instance, the FCA could focus on an individual firm with high-risk or PEP customer shares exceeding these industry-wide averages or, on the other hand, falling significantly below what might be expected for a firm of that size (and therefore potentially evidencing inadequate identification of high-risk customers). Adequate identification and management of high-risk customers has remained a key focus in the FCA’s 2017/18 annual report, with enforcement activity taken in June 2018 against Canara Bank.

### Current industry activity in tackling financial crime

There are two key themes arising from the data provided in the return:

- **Resourcing costs:** Combatting financial crime continues to impose a heavy compliance resourcing cost on the UK financial services industry. Based on the survey results, over GBP650m is spent per year in “dedicated staff time to combat fraud, laundering and other financial crimes”, with collective employment of 11,500 full-time staff in financial crime roles. The actual costs incurred were acknowledged by the FCA to likely be significantly higher when accounting for support costs such as information technology expenditure.

- **Suspicious activity reporting and interaction with law enforcement:** the Money Laundering Reporting Officers within the surveyed firms handled 923,000 internally escalated suspicious cases in the 12-month reporting period. Following investigations, 363,000 suspicious activity reports (almost 40%) were then filed externally by firms with the UK National Crime Agency (the NCA), together with over 2,100 terrorism-related suspicious activity reports.

In terms of the information flow in the other direction, law enforcement agencies submitted 123,000 investigative orders in the reporting period and imposed 16,000 restraint orders (only a quarter of which were new) on bank accounts to freeze funds suspected of containing criminal property. Only a small percentage (approximately 1%) of SARs filed with the NCA resulted in the NCA taking enforcement action, in possible evidence of ‘over reporting’ within the sector.
The OECD has criticised the UK for the low level of corruption enforcement activity resulting from the current SARs regime. Given the large volume of SARs filed on a daily basis, and many being of ‘low quality’, investigation authorities face a challenge in detecting where the real risks lie. The large volume also indicates a tendency in the financial services sector to over report suspicions.

**Industry perceptions of risks: cybercrime at the forefront**

As part of the survey, firms were asked about the type of fraud risk they considered to be of highest concern. The top two risks may come as little surprise: identity fraud/identity theft and phishing were of top concern across the industry following high-profile attacks and press coverage. While these and other frauds enabled by new technology (such as hacking and malware-enabled fraud) were widely perceived by firms to be rising both in volume and as a matter of concern, firms also remained focused on long-established forms of crime including account takeover, application fraud and card fraud.

The report has been followed by a further FCA report on Cyber and Technology Resilience: Themes from cross-sector survey 2017 – 2018. On 27 November 2018, Megan Butler, Executive Director of Supervision at the FCA, warned that the FCA saw “no immediate end in sight” to the rise in cyber attacks affecting UK financial services. She continued that “all the trends […] suggest an increasing threat to UK customers, and financial markets”. Firms reported an 18% increase in cyber incidents in the year ending October 2018, but Butler noted that underreporting is likely still an issue and that some businesses may not appreciate the level of risk posed by cyber attacks.

The FCA has shown a particular interest in combatting cyber risks by emphasising (and enforcing) the need to implement appropriate systems and controls. In its recent Cyber and Technology Resilience report, the FCA confirmed that, pursuant to Principle 11 of the FCA Handbook, financial services firms are expected to report “major technology outages and cyber-attacks”. A firm should therefore consider whether any cyber crime incident is ‘material’, namely whether it affects a large number of customers and/or results in significant loss of data, availability or control of the firm’s IT systems, unauthorised access to information and communication systems or malicious software on those systems. In such cases, the firm should report the cyber crime to the relevant regulators within an appropriate timeframe.

In relation to country risk, Iran, Panama and Russia were the three countries most often classified as ‘high risk’ by surveyed firms based on the risk of financial crime, followed by Iraq and Laos. The FCA emphasised that the industry rankings of country risk based on the survey results do not reflect the FCA’s views and may be of limited application, given that some firms may not have performed a risk assessment of certain jurisdictions. Despite this caveat, when viewed alongside other publicly available indexes relating to jurisdictional risk, for example the Transparency International’s Corruption Perceptions Index, firms may find this useful guidance on the general views taken by their peers on country risk.

**What is this likely to mean in terms of regulatory focus in 2019?**

The FCA expects that this financial crime report data will allow it to more accurately identify firms with the highest exposure to money laundering risks. It can therefore target its resources to prevent the most harm to the UK’s financial markets. Rob Grippetta, Head of the Financial Crime Department at the FCA, explained in a speech on 19 November 2018 that the FCA is moving to a “more data-driven, predictive place” where it has “started experimenting” with “supervised supervision” of firms. The annual return data can be combined with other data about firms to identify those firms with areas of particular strength or weakness, which could potentially be replicated or remediated throughout the industry.
This report reflects only the first year of data collected from the UK financial services industry and it is by its nature difficult to obtain accurate figures on financial crime. However, the trends and common concerns should assist UK (and perhaps European) firms in benchmarking their views and potentially improving their monitoring and prevention of financial crime. Although the FCA collected data only within the UK, the results may reflect wider trends at a European level.

For instance, the European Banking Authority’s recent risk assessment, published in December 2018, highlighted that almost 90% of EU banks reported cyber risks and data security as key operational risk drivers, a rise from 55% in 2017. Gruppetta also noted in his speech that the financial crime report provides an opportunity for regulators to benchmark their views against industry-wide perceptions. As the data pool grows each year, we hope to identify possible future industry drivers from the patterns that emerge.

Stacey McEvoy, Senior Associate, and Bethany Gregory, Trainee Solicitor, London

---

**Settlement**

**FRANCE**

Renowned French businessman pleads guilty to settle misuse of corporate assets charges

In the investigation against a former presidential candidate, a renowned French business man has pleaded guilty in order to settle misuse of corporate assets charges.

He admitted to having paid the former presidential candidate’s wife an excessive salary and also a fictitious salary. He accepted an eight-month prison sentence (entirely suspended) and a EUR375,000 fine.

This guilty plea mechanism amounts to an admission of guilt, constituting a criminal conviction which will feature on his criminal record.
Cybercrime

FRANCE

Major French company is victim of CEO fraud

In the Q3 2018 edition of the WCCR we reported on the CEO Fraud investigation concerning a former French Minister of Defence. Since then, the French press has revealed that a major French company has also fallen victim to CEO Fraud, amounting to more than EUR19m.

In March 2018, fraudsters are alleged to have impersonated the directors of the French company’s head office and persuaded the CEO and CFO of its subsidiary in the Netherlands to transfer funds for an alleged acquisition in Dubai.

Sanctions

FRANCE

French Senate Committee adopts a European resolution on the extraterritoriality of American sanctions

On 12 November 2018, the Commission in charge of European affairs (part of the French Senate) adopted a European resolution on the extraterritoriality of American sanctions.

The resolution notes that such sanctions jeopardise the diplomatic and economic sovereignty of the EU and its Member States. It focuses on (i) the legal and financial measures which could be used to block or neutralise extraterritorial American sanctions, (ii) the decisions which could be taken to strengthen the role of the Euro on an international level, and (iii) the political steps which could be taken in support of the EU’s positions on the extraterritoriality of American sanctions. At this stage, the resolution simply shows political willingness on the part of France to take action with the EU as regards the extraterritoriality of American sanctions.
The Senior Director for Antitrust Enforcement of the Competition and Markets Authority, Ann Pope, gave a speech in late 2018 on its competition enforcement work to date and what lies ahead.

Ms Pope discussed the increase in the CMA’s enforcement activity, both in terms of cases opened and infringement decisions taken. In particular, she noted the progress in using Competition Disqualification Orders, whereby an individual is disqualified from being a director of a UK company for up to 15 years as a result of their involvement in a competition law infringement. In 2018, the CMA secured the disqualification of two directors involved in an estate agency cartel, for three and three and a half years respectively, bringing the total of Competition Disqualification Orders up to three. Whilst still in their infancy, Ms Pope warned that such orders would not be the last and that the CMA would continue to use these powers to ensure directors and managers are held personally liable for corporate breaches of competition law.

Ms Pope also looked at the challenges and opportunities arising out of Brexit. The CMA has been actively preparing and releasing guidance outlining the agency’s role in merger, state aid and competition law enforcement after Brexit, including under a no deal scenario.

Other challenges facing the CMA have little to do with Brexit – combatting how long cases take, the increase in legal challenges to the agency and low competition law awareness among businesses. In light of the proposed reform of the CMA’s remit, discussed below, it looks as though some changes are on the cards.

Proposed reform of CMA’s remit: mandatory notification of larger mergers, consumer law and enhanced CMA toolkit

On 25 February the Competition and Markets Authority (CMA) published its preliminary proposals for legislative and institutional reforms to competition and consumer protection law and policy. The proposals if implemented have the potential to change significantly the balance of enforcement enabling a more interventionist stance by the CMA in the regulation of markets and merger activity.

In summary, in response to concerns about its ability to tackle effectively existing and new forms of consumer harm, it is proposed that the CMA be given new duties and responsibilities relating to consumers together with new tools and powers to support those duties and responsibilities, including to facilitate the use of interim measures. To help the CMA focus more effectively on its core responsibilities, it is proposed that the CMA transfer some of its existing powers and functions to other bodies, for example in the field of regulatory appeals and criminal cartel enforcement. One of the key changes proposed (and not for the first time) is a mandatory and suspensory notification of certain mergers. We set out below some of the key proposals in further detail.

Mandatory merger regime on the cards

The CMA Chairman, Lord Tyrie notes that whether or not there is a deal on Brexit, further changes to the procedural framework, the statutory timetable and the decision-making structures for merger control are likely to be needed. In particular, “for the UK to ensure that it has appropriate influence” and to protect consumers, he proposes mandatory notification to the CMA of mergers above a threshold set at a level to catch larger mergers that are typically reviewed by multiple international competition authorities, accompanied by a “standstill

© Allen & Overy LLP 2019
provision” designed to prevent parties from proceeding with the transaction prior to CMA approval as it is the case in the majority of other jurisdictions including the U.S., the EU and most Member States. Although not clear in the proposals, the CMA also considers that there may be merit in introducing reporting mechanisms for certain businesses so that they are required to inform the CMA of mergers and acquisitions they undertake, and giving the CMA an opportunity to “call in” merger activity. Whilst in practice most large mergers that fall under the jurisdiction of the CMA are in any event notified, if this proposal is implemented acquirers would no longer be able to take the antitrust risk and close pending notification.

**Consumer protection at centre of proposals, particularly in the digital economy**

It is proposed that the economic interest of consumers, and their protection from detriment, be made a paramount overriding statutory duty not only of the CMA but also the courts (including the Competition Appeal Tribunal (CAT)). This is not a purely academic debate. It would have practical implications. The expectation is that, together with further new duties, including for the CMA to conduct its investigations swiftly while respecting parties’ rights of defence, the CMA will be better armed to address quickly and effectively novel and emerging forms of consumer detriment, particularly in digital markets, and to protect vulnerable consumers.

**A more effective and flexible markets regime**

The UK is one of the few jurisdictions worldwide where the CMA can intervene in relation to markets to investigate whether they are functioning appropriately in the absence of a breach of competition law. The CMA has done so on a number of occasions in relation to banking, energy and airports to name just a few examples. The CMA wants to improve its ability to intervene and take action.

Recommendations to improve the regime for market studies and market investigations include:

- aligning the scope of phase 2 market investigations more closely with phase 1 market studies to enable the CMA to order legally enforceable remedies to address consumer detriment without having to demonstrate an adverse effect on competition;
- for breach of such undertakings; and
- empowering the CMA to fine firms that fail to comply with remedies ordered.

**Enhanced powers for enforcement generally**

**Individual responsibility**

Criminal hard-core cartel provisions have been invoked rarely by the CMA and the CMA takes the view that personal responsibility for competition law compliance could be bolstered “if the CMA were able to impose individual fines directly on individuals for serious competition law infringements”. Lord Tyrie notes, however, that a good deal of further work would be required to assess the merits of such a change. And he believes the case for giving responsibility for cartel prosecution to an agency that routinely brings criminal prosecutions, such as the Serious Fraud Office, merits reconsideration.

The CMA also advocates the consideration of measures to establish a clear line of responsibility to the boards of public companies for competition and consumer law compliance, including a requirement to appoint a board director with responsibility for assessing and reporting on relevant compliance risks and a requirement on auditors to make a report to the company if, during the course of their usual work, they identify practices that may raise compliance risks, with a corresponding duty on company directors to attest in annual reports that these risks have been noted and addressed.

**Whistleblowers**

Noting the value of whistleblowers to the CMA’s work, the CMA advocates giving whistleblowers far greater financial compensation (currently limited to GBP100,000) and stronger protections of confidentiality, together with a requirement on auditors to report suspected infringements of competition law identified during the course of their usual work to the CMA and the Financial Reporting Council.

**Investigatory and information-gathering powers**

In the CMA’s view:

- a turnover-based fines regime for non-compliance with both competition and consumer protection law enforcement investigations is almost certainly required;
- civil fines for the provision of false or misleading information are needed;
- the CMA could be made subject to an explicit statutory requirement to conduct its investigations swiftly, while giving due consideration to parties’ rights of defence;
- empowering the CMA to itself decide whether consumer protection law has been broken, declare the fact publicly, direct businesses to bring infringements to an end and impose fines, with fines applying also for breach of undertakings provided to the CMA;
– giving the CMA the ability to impose legally enforceable requirements on firms on an interim basis, pending the completion of its full market investigations;
– allowing the CMA to accept undertakings at any time before or during a market study, and to fine firms
– a general power to require information to be produced could assist in the identification and response to problems in fast-moving markets; and
– further consideration should be given to whether information-gathering powers are sufficiently effective to investigate companies located outside the UK.

Court review of CMA decisions
The CMA feels that its efforts to tackle consumer harm are dampened by an excessively heavy judicial oversight which absorbs a large degree of resources in defending cases and, indirectly, at the investigative stage. Whilst accepting that judicial oversight is important, the CMA proposes:
– moving from the current “full merits” standard of review either to a judicial review standard or to a new standard of review, setting out specified grounds of permissible appeal; and
– amending the CAT’s rules of procedure to restrict admissibility of new evidence and place less reliance on oral testimony.

An enhanced consumer law enforcement toolkit
Finally the CMA is proposing to add more teeth to its consumer protection powers. Lord Tyrie states that “the CMA’s consumer law powers are unfit for its current purpose, and far short of what would be required to enable the CMA effectively to fulfil a consumer interest duty” and that “deterrence, in short, is very limited”. He suggests:

– enabling the CMA, in urgent cases, to order the cessation of practices that it suspects may be harming consumers on an interim basis, pending a final decision on whether the law has been broken;
– introducing director disqualification provisions for more serious breaches of consumer protection law; and
– entrenching a division of responsibilities for consumer law enforcement between the CMA and Trading Standards in law.

The majority of the CMA’s proposals will require further, often extensive, work, and we expect to see more detailed proposals put out to wider consultation including as part of the Government’s review of the competition regime. We will closely follow developments and responses.


Mark Friend, Partner, Philip Mansfield, Partner, Antonio Bavasso, Partner, Dominic Long, Partner, Alasdair Balfour, Partner, London
Other developments

GERMANY

Developments in German emissions scandal

- German car manufacturer linked to diesel emissions scandal offers to pay a fine of EUR800m: A major German car manufacturer linked to the diesel emissions scandal has accepted the Public Prosecutor’s penalty notice amounting to a fine of EUR800 million in return for the Public Prosecutor’s Office in Munich terminating its administrative offence proceedings – but the investigations continue. The amount is payable with regard to accusations of manipulation of vehicles with V6 and V8 diesel engines. According to a statement of the car manufacturer, it accepted the fine imposed by the Public Prosecutor’s Office in Munich and thereby admitted its responsibility.

- Indictment of former manager of German car manufacturer: According to press reports, the Public Prosecutor’s Office in Munich is preparing to indict a former manager of a major German car manufacturer linked to the diesel emissions scandal. The core accusation is that the former manager prevented rapid escalation of issues once they had been discovered and issued false documents.

UK

National Economic Crime Centre launched

The NCA has announced the launch of the National Economic Crime Centre (NECC), the national authority for the UK’s operational response to economic crime. The multi-agency NECC, which commenced operations on 31 October 2018, forms part of the UK government’s wider five year Anti-Corruption strategy. Its function is to strengthen the UK’s ability to fight economic crime, with a particular focus on money laundering and corruption offences, through greater inter-agency cooperation.

Describing itself as a “partnership”, the NECC will coordinate and prioritise activity, resources and intelligence-sharing domestically and internationally across different prosecutorial bodies and law enforcement agencies, as well as governments and the private sector. With around 55 staff, it will sit within the same building as the NCA, and work in conjunction with the SFO, FCA, CPS, HMRC and the City of London Police. Since assuming her role as Director of the SFO, Lisa Osofsky has stressed the importance she placed on working across agencies in order to achieve results.

The NECC is no different and Osofsky sees the SFO and HMRC as natural allies, capable of building “very strong” cases together.

While the SFO will remain a stand-alone agency, the NECC has powers to ‘direct’ the SFO to conduct investigations, which may in due course raise questions over its continued independence. There is no sign of a merger between the SFO and NCA despite the plans set out in the 2017 conservative manifesto, but Osofsky has placed a greater emphasis on cooperation as an important strategic focus. The NECC will also promote the use of new powers such as Unexplained Wealth Orders and Account Freezing Orders.
A closer look: Romania: *Venice Commission expresses concerns over proposed amendments to two criminal codes*

In order to implement the relevant Constitutional Court – decisions and EU Directives, a reform of the Romanian criminal codes is required.

In this context, on 20 October 2018 the Venice Commission published a report on the proposed amendments to the Criminal Code and the Criminal Procedure Code in which it criticised a number of the proposals as being in conflict with Romania’s international obligations (especially regarding the fight against corruption) and going far beyond the requirements resulting from the case law of the Constitutional Court.

The Venice Commission also indicated that the reform was inadequate, and did not constitute a comprehensive review of two of the most important and sensitive codes; the amendments under review were adopted in a legislative process which was excessively fast and lacking in transparency.

As far as the Criminal Code is concerned, the following provisions, among others, have been the focus of criticism and are now subject to possible re-assessment by the legislature:

- **Extended confiscation measures** – this proposed amendment would require the court to use the ‘beyond any reasonable doubt’ standard when determining whether to order the extended confiscation of assets. The Venice Commission indicated that courts will rarely rule in favour of extended confiscation as in most cases, the prosecution will be unable to prove beyond any reasonable doubt that the value of assets held by the accused clearly exceeds the revenue obtained lawfully by them, therefore casting doubt on whether the assets originate from criminal activities.

- **Statute of limitations** – the Venice Commission noted that the envisaged amendment referring to the reduction of the statute of limitations periods will in particular affect corruption offences and that such limitation raises serious concerns both with respect to the rule of law in general and the country’s respect for its international obligations in particular.

Bribery – this amendment proposes that a briber will be ‘forgiven’ if he/she reports the crime within one year of the action being carried out. The Venice Commission held that this amendment will discourage bribers from cooperating with law enforcement agencies post the one year mark and make it much harder to uncover (and consequently to prosecute and to prove) corruption offences.

- **Embezzlement** – the proposed modification is that ex officio investigations will no longer be possible for this offence. As a result: (i) the criminal proceedings in cases of embezzlement should be initiated only following a criminal complaint and (ii) the reconciliation between the involved parties should result in the removal of criminal liability. The Venice Commission recommended the removal of such modification.

As far as the Criminal Procedure Code is concerned, the Venice Commission has criticised, among others, the following provisions:

- **Initiation of criminal investigations** – the proposed amendment introduces a maximum period of one year from the beginning of an in rem criminal investigation during which the criminal investigation in personam must commence, or the case has to be closed. The Venice Commission held that a one-year time limit for investigating alleged crimes, regardless of the nature of the offence and the degree of complexity of the case, appears to be too a short period of time, especially with regard to large and complex cases involving serious crimes. The key concern is that this new time bar may lead to a large number of criminal cases being closed.

In light of the above, the Venice Commission recommended that the Romanian authorities conduct an overall re-assessment of the amendments to the two codes, through a comprehensive and effective consultation process, in order to devise a solid and coherent legislative proposal benefiting from broad support within Romanian society and fully taking into account the applicable international and constitutional standards.

*Ana Popa (Nedelcu), Associate, Adrian Cristea – Associate, RTPR Allen & Overy Bucharest*
## Looking ahead

<table>
<thead>
<tr>
<th>Date</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BELGIUM</strong></td>
<td></td>
</tr>
<tr>
<td>31 March 2019</td>
<td>Belgian companies and other relevant legal entities to complete the UBO Register.</td>
</tr>
<tr>
<td><strong>FRANCE</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the context of the bill on the growth and transformation of businesses, an amendment presented by the French Government has been adopted by the French Parliament, in order to allow the Government to transpose the 5th AML Directive into French law and amend chapters of the Monetary and Financial Code regarding asset freezing, through orders (ordinances), thereby avoiding lengthy parliamentary debates.</td>
</tr>
<tr>
<td><strong>ROMANIA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Probably during the second part of 2019</td>
</tr>
<tr>
<td></td>
<td>Adoption of the law implementing 4MLD.</td>
</tr>
<tr>
<td><strong>UK</strong></td>
<td></td>
</tr>
<tr>
<td>29 March 2019</td>
<td>The UK continues to publish Statutory Instruments seeking to ensure that European legislation is onshored by exit day.</td>
</tr>
</tbody>
</table>
Contributors and key contacts

Editorial team

Hayley Humphries (UK)
hayley.humphries@allenovery.com

Contributors to this edition

Czech Republic: Markéta Císařová; Michal Zabadal
France: Dan Bengaigui; Marine Gourlet; Rebecca Harris
Germany: Gero Pogrzeba; David Schmid
Luxembourg: Thomas Berger
Netherlands: Neyah van der Aa; Jurian van Galen
Poland: Bartosz Marczyński; Monika Muraw ska; Marek Neumann
Romania: Adriana Dobre; Ana Popa, Adrian Cristea, Petruș Partene
Spain: Lara Ruiz
UK: Claudia Barry; Armondo Chakrabarti; Nicole Choong; Amy Edwards; Eve Giles; Bethany Gregory; Natalie Kaminoki; Stacey McEvoy; Jason Rix; David Siesage; Sophie Walker

Key contacts by jurisdiction

Belgium
Joost Everaert, joost.everaert@allenovery.com
Nanyi Kaluma, nanyi.kaluma@allenovery.com

Czech Republic
Markéta Císařová, marketa.cisarovva@allenovery.com

France
Dan Bengaigui, dan.bengaigui@allenovery.com
Denis Chemla, denis.chemla@allenovery.com
Hippolyte Maquerty, hippolyte.maquerty@allenovery.com

Germany
Wolf Bussian, wolfgang.bussian@allenovery.com

Hungary
Balázs Sahin-Tóth, balazs.sahin-toth@allenovery.com

Italy
Massimo Greco, massimo.greco@allenovery.com
Amedeo Sada, amedeo.sada@AllenOvery.com

Luxembourg
Thomas Berger, thomas.berger@allenovery.com

Netherlands
Hendrik Jan Biemond, hendrikjan.biemond@allenovery.com

Poland
Jaroslaw Iwanczyki, jaroslaw.iwanczyki@allenovery.com
Marek Neumann, marek.neumann@allenovery.com
Kryszyna Szczepanska-Kozlow ska, kryszyna.szczepanska-kozlow ska@allenovery.com

Romania
Valentin Bera, valentin.bera@rtprallenovory.com
Adrian Cristea, adrian.cristea@rtprallenovory.com

Slovakia
Martin Magil, martin.magil@allenovery.com

Spain
Javier Castresana, javier.castresana@allenovery.com
Antonio Vazquez-Guillen, antonio.vazquezguillen@allenovery.com

UK
Calum Burnett, calum.burnett@allenovery.com
Law son Caisley, lawson.caisley@allenovery.com
Armondo Chakrabarti, armondo.chakrabarti@allenovery.com
Eve Giles, eve.giles@allenovery.com
Jonathan Hitchin, jonathan.hitchin@allenovery.com
Our European white collar crime practice

As part of Allen & Overy LLP’s market-leading global investigations practice, our European white collar crime experts advise clients on a wide range of high-profile criminal and regulatory investigations, with a particular focus on cross-border matters. The European team comprises lawyers with extensive experience of working together in multiple jurisdictions and includes former prosecutors in Europe.

To find out more, visit: allenover.eye.com

“With a scale and depth of expertise that few firms can match — in the UK or globally — Allen & Overy’s investigations specialists are frequently found on the world’s largest and most complex matters.”

Global Investigations Review, the GIR 30, 2016

"Their commitment to excellence and client service is second to none."

Chambers 2019, Corporate Investigations — Global-wide

“Allen & Overy delivers top-notch work.”

Chambers 2017, Corporate Investigations — Europe-wide

To receive regular copies of our European White Collar Crime Report directly to your inbox, please email:

litigationpublications@allenover.eye.com
GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,500 people, including some 550 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

- Abu Dhabi
- Amsterdam
- Antwerp
- Bangkok
- Barcelona
- Beijing
- Belfast
- Bratislava
- Brussels
- Bucharest (associated office)
- Budapest
- Casablanca
- Doha
- Dubai
- Düsseldorf
-Frankfurt
-Hamburg
-Hanoi

- Ho Chi Minh City
- Hong Kong
-Istanbul
-Jakarta (associated office)
-Johannesburg
-London
-Luxembourg
-Madrid
-Milan

- Moscow
-Munich
-New York
-Paris
-Perth
-Prague
-Riyadh (cooperation office)
-Rome
-São Paulo

- Seoul
-Shanghai
-Singapore
-Sydney
-Tokyo
-Warsaw
-Washington, D.C.
-Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP’s affiliated undertakings.

© Allen & Overy LLP 2019 | BS:13000631.4