GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume I: Global Investigations in the United Kingdom and the United States

SIXTH EDITION

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo, Michael Bowes QC, Luke Tolaini, Ama A Adams, Tara McGrath

2021

2

Europe Overview

Robert Dalling, Kelly Hagedorn and Matthew Worby[1]

Introduction

The European investigations landscape is characterised by a patchwork of varying legislative and regulatory frameworks and enforcement approaches. These are often shaped by past events and current political priorities in particular jurisdictions. These variations and the pace of change mean that cross-border investigations, whether involving multiple European jurisdictions or parallel investigations by enforcement authorities in other regions (or sometimes both), frequently present thorny practical and tactical challenges.

This overview does not seek to duplicate the commentary and analysis set out in many of the chapters in this volume. Rather, it looks at some of the key priorities of European enforcement authorities, focusing on anti-bribery and corruption, anti-money laundering, tax evasion and data protection. There is significant ongoing activity in these areas, and some authorities are adapting their approaches to make effective use of changes in the law and additions to their toolkits. This overview also looks ahead to seek to identify the key issues and trends on which those who are subject to investigations throughout Europe should be focusing.

Areas of enforcement risk

Anti-bribery and corruption

A substantial number of investigations by enforcement authorities have arisen following significant legislative developments that introduced corporate offences of failure to prevent bribery with extraterritorial effect (such as the UK Bribery Act 2010 (UKBA) and France's Sapin II Law). These legislative developments have been accompanied by new mechanisms enabling criminal investigations that involve corporate organisations

1 Robert Dalling and Kelly Hagedorn are partners and Matthew Worby is an associate at Jenner & Block London LLP.

to be concluded through negotiated settlements. To date in Europe, these mechanisms have been used mainly (although not exclusively) in cases concerning historic bribery and corruption involving corporate organisations.

Following these developments, and despite a slow start, there has been increasing pressure for corporate criminal liability to be expanded to encompass other financial offences. The UK government, for example, commissioned a consultation in 2021 on the extent to which corporate criminal liability should be further reformed in England and Wales.[2]

Several other jurisdictions have introduced anti-bribery legislation in recent years, some of which has been the subject of criticism. In Ireland, for example, an offence analogous to the UK corporate offence of failure to prevent bribery came into force in July 2018.[3] However, the Irish statute has been described as flawed for failing to meet guidelines published by the Organisation for Economic Co-operation and Development (OECD). This is because the Irish statute requires dual criminality for an offence to be committed overseas.[4] Further, there is no guidance akin to that published by the UK Ministry of Justice in relation to 'adequate procedures' under the UKBA. There is therefore some remaining uncertainty among corporate organisations and their advisers as to exactly what 'taken all reasonable steps and exercised all due diligence' means in the Irish legislation, and how to avail oneself of a defence to the corporate offence. Given the nature of the Irish economy, and in particular its attractiveness to multinational technology and financial services companies, there is potential for investigations in Ireland to have significant cross-border elements, and clarity on this point would be welcome.

Elsewhere, German criminal law does not currently recognise the concept of corporate criminal liability. Although the German government introduced draft legislation in this area in August 2019, the legislation was not passed before the end of the same legislative session. As a result, the German government will need to reintroduce the draft legislation after the federal elections in September 2021 if it is to become law. It is unclear whether there is any appetite to do so.[5] In Poland, the OECD has described delays to legislation amending liability under Polish law for legal persons, and increasing financial penalties against corporations, as 'a serious concern'. It unclear whether the Polish government will enact any reform.[6]

2 https://consult.justice.gov.uk/digital-communications/corporate-liability-for-economic-crime/.

3 Ireland: Criminal Justice (Corporate Offences) Act 2018.

4 'Irish corruption law not in compliance with OECD guidelines', *The Irish Times* (26 August 2019), at https://www.irishtimes.com/news/crime-and-law/irish-corruption-law-not-in-compliance-with-oecd-guidelines-1.3997012.

5 'German corporate criminal liability reforms left in limbo', *Global Investigations Review* (2 July 2021), at https://globalinvestigationsreview.com/anti-corruption/german-corporate-criminal-liability-reforms-left-in-limbo.

6 'Poland's lack of progress in implementing reforms to boost fight against foreign bribery remains a serious concern' (22 June 2021), at https://www.oecd.org/poland/poland-s-lack-of-progress-in-implementing-reforms-to-boost-fight-against-foreign-bribery-remains-a-serious-concern.htm.

Anti-money laundering

Although anti-money laundering (AML) enforcement remains high on most enforcement authorities' agenda, approaches to, and the resources available for, investigations vary considerably between European jurisdictions. This is despite the introduction of various iterations of the EU Money Laundering Directives (MLDs), which aim to standardise this area of enforcement. The latest MLD was the sixth, which EU Member States were due to implement by 3 December 2020. The sixth MLD seeks to regularise further the AML enforcement landscape in Europe, for example by:

- standardising the 22 predicate offences that must be considered 'criminal activity' for the purposes of money laundering by EU Member States;
- requiring EU Member States to expand criminal liability for money laundering to legal persons; and
- setting certain increased EU-wide minimum penalties for money laundering.

Although the effect of the sixth MLD is yet to be fully felt, enforcement action across Europe has continued apace. Some of the highest penalties imposed in recent years have resulted from investigations by Sweden's Financial Supervisory Authority[7] and the Netherlands' Public Prosecution Service.[8] These fines were issued for breaches of regulatory requirements and criminal law by major institutions in relation to their AML systems and controls. This marks a change, since France and the United Kingdom have historically imposed the heaviest fines in the region for AML-related transgressions. That is not to say that France's AML-related enforcement has not remained effective. The Autorité de Contrôle Prudentiel et de Résolution has reportedly focused in 2020 on smaller financial institutions, including payment service providers, rather than larger banks and money services businesses.

Fines are not the only notable feature of enforcement activity in this area. First, reflecting an increasingly close focus on individual accountability, regulators are now ready and able to pursue individuals considered to have played a part in AML failings. Second, it would appear that some European regulators are starting to initiate criminal prosecutions for this conduct at a corporate level. In 2021, the UK Financial Conduct Authority (FCA), for example, initiated its first criminal prosecution of a major financial institution for allegedly failing to prevent money laundering. It remains to be seen whether this prosecution will be successful, and the extent to which non-monetary penalties, such as reputational damage, will influence the approach of financial institutions in the future.

Tax evasion

Tax evasion is also increasingly attracting authorities' attention. In particular, several jurisdictions are seeking to prosecute a trading activity, known as cum-ex trading, whereby banks and stockbrokers engage in trading shares in a manner that allows both sides of a transaction to claim a tax rebate on the dividends purportedly paid by the shares.

7 Sweden: Swedbank was fined US$386 million for compliance deficiencies relating to Baltic money laundering, and Skandinaviska Enskilda Banken was fined €95 million for similar conduct.

8 Netherlands: ING Groep was fined US$900 million for broad failures relating to financial crime compliance controls.

Germany is the most prominent example, where an estimated €31.8 billion was fraudulently claimed from the government in the form of rebates between 2001 and 2016.[9] It has been estimated that the total cost to the European taxpayer is more than €55 billion between 2001 and 2012.[10]

Enforcement action in response to such long-standing and wide-ranging conduct is complex, but has enjoyed some success. The Danish tax authority (SKAT), for example, charged three UK nationals and three US nationals for their role in allegedly defrauding the Danish treasury.[11] At least one former executive of a private bank in Germany has been sentenced to five and a half years for similar conduct, and two British nationals received suspended sentences in Germany.[12] However, enforcement action in response to this activity has not been entirely successful. Denmark, for example, is currently seeking to appeal a UK High Court decision ruling that SKAT cannot pursue a lawsuit seeking to recover £1.5 billion in the English courts.

More generally, the impact of fraud on the support measures introduced by various governments in response to the coronavirus pandemic has been well publicised. The UK government has announced an investment of £100 million in a Taxpayer Protection Taskforce to recover funds paid out incorrectly or as a result of fraud during the pandemic.[13] We anticipate other European jurisdictions will take a similar approach.

Data protection

The General Data Protection Regulation (GDPR) is now three years old and several themes are emerging. Following Brexit, we are yet to see any substantive divergence by the United Kingdom away from the GDPR, probably because of the UK's need to obtain an adequacy decision in respect of its data protection legislation, which it duly received in June 2021. Now that this decision has been obtained, potential divergence by the United Kingdom is a trend to watch for in 2022, as the UK government starts to consider how best to approach the digital economy and data protection outside the European Union.

The most significant trend we have seen thus far is the willingness of European data protection authorities to enforce the GDPR aggressively. A total of 880 fines have been

9 'Cum-ex tax scandal cost European treasuries €55 billion', DW Akademie (18 October 2018), at https://www.dw.com/en/cum-ex-tax-scandal-cost-european-treasuries-55-billion/a-45935370.

10 The Cum-ex files (information document), European Parliament, at https://www.europarl.europa.eu/cmsdata/158435/2018-11-26%20-%20Information%20paper%20on%20Cum-ex%20-%20Cum-cum.pdf.

11 'Dividend Reclaim Case: Six persons formally charged with defrauding the Danish Treasury of more than DKK 1 billion', Anklagemyndigheden, at https://anklagemyndigheden.dk/sites/default/files/inline-files/2096_PM_Udbyttesagen_North%20Channel%20Bank_EN.pdf.

12 'Banker first to be jailed in German tax fraud scandal', Reuters (1 June 2021), at https://www.reuters.com/legal/transactional/banker-first-be-jailed-german-tax-fraud-scandal-2021-06-01/.

13 'COVID-19: how HMRC will continue to support customers and the economy', HM Revenue and Customs, at https://www.gov.uk/government/publications/hmrc-issue-briefing-how-hmrc-will-continue-to-support-customers-and-the-economy/covid-19-how-hmrc-will-continue-to-support-customers-and-the-economy.

issued, or declared, for a cumulative total of €1,291,357,143.[14] The largest fines have also been significant. Amazon may be fined up to €746 million by Luxembourg's data protection authority (at the time of writing the fine had been issued but was still subject to challenge by Amazon), and Google Inc was fined €50 million by the French data protection authority in 2019.

A developing trend of note is the role that non-governmental organisations have played in initiating data protection enforcement actions in the European Union. For example, La Quadrature du Net and None of Your Business (NOYB), French and Austrian pressure groups respectively, have reportedly filed (either collectively or individually) complaints that prompted the enforcement actions against Amazon and Google mentioned above. In addition to filing complaints, pressure groups are also litigating data protection issues directly. NOYB, through its leader Max Schrems, conducted the litigation that resulted in the US–EU Privacy Shield being declared invalid, and the Dutch pressure group Privacy Collective is reportedly suing Salesforce and Oracle in a class action targeting the cookie-tracking practices deployed by both companies. Corporates should therefore be aware that oversight of their data protection practices may be undertaken by civil society, not just regulators, and that those grievances may be taken to court.

Beyond the increasing importance of data protection as a risk area for corporates, investigators must now also keep data protection issues in mind when tackling a cross-border investigation. In particular, issues arising from the international transfer of personal data are becoming increasingly difficult globally, not just in Europe.

Increased pressure and incentives to co-operate

In England and Wales, the body of cases in which deferred prosecution agreements (DPAs) have been concluded between the Serious Fraud Office (SFO) and co-operating corporate organisations is slowly growing. Although the figure of 20 agreements per year predicted during the passage of the legislation that introduced DPAs seems unlikely to be achieved in the near term, the SFO entered into three DPAs in 2020 and three in 2021 (so far). This is the highest annual total for the SFO since the introduction of DPAs in the United Kingdom. Despite this increase, the SFO has itself been under pressure, having failed to date to secure the conviction of any individual named as an alleged offender in any of the DPAs. Against this backdrop, it remains to be seen whether the UK DPA regime will be considered a success, and if corporates will consider co-operation to be worthwhile. The SFO may also find itself under increasing scrutiny after it was revealed that the agency's enforcement activity has been markedly reduced during the coronavirus pandemic.

In France, the authorities responsible for investigating and prosecuting financial crime, the French Anti-Corruption Agency (AFA) and the National Financial Prosecutor's Office (PNF), have now concluded 13 published judicial public interest agreements (CJIPs)[15] with companies of various sizes, including one in which the global penalties imposed exceeded US$3.9 billion. A recent example also indicates that co-operation with

14 As at 4 October 2021. This figure includes notices of an intention to fine and so may be subject to change – see https://www.privacyaffairs.com/gdpr-fines/.

15 https://www.agence-francaise-anticorruption.gouv.fr/fr/convention-judiciaire-dinteret-public.

the French authorities can result in a significant reduction in penalty. Systra, a transport company, saw its theoretical potential fine of €187 million ultimately levied at €7.5 million after the French authorities viewed the comprehensive compliance programme, in conjunction with historic offending, favourably.[16]

It remains to be seen whether further jurisdictions will enact similar measures. A November 2020 report published by the Irish government as part of measures to enhance Ireland's ability to fight economic crime declined to recommend the introduction of a deferred prosecution regime. In their report, the authors stated that they were 'not convinced that the introduction of a DPA regime will yield any significant benefit given the UK experience so far'.[17]

Although mechanisms similar to DPAs and CJIPs (or aspects of them) exist in some other jurisdictions around Europe, including Belgium, the Czech Republic, Romania and Slovakia, they are available only in some of these jurisdictions to resolve allegations of corruption, and the practice and procedure around the use of those mechanisms is not always clearly set out. It is also unclear whether any of these jurisdictions wish to expand these mechanisms. Concluded cases of the same magnitude as those seen in the United Kingdom and France have yet to be publicised.

The different approaches of European jurisdictions should be considered when dealing with global settlements. The Dutch company VEON, for example, entered into a joint global settlement with Dutch and US authorities to resolve an enforcement action under the US Foreign Corrupt Practices Act (FCPA), whereas Ericsson became the subject of an investigation by the Swedish authorities shortly after reaching a settlement to resolve an FCPA action with the US authorities.

In jurisdictions where DPAs are already established, authorities' and courts' expectations of co-operating corporate organisations in order for (1) negotiations to take place and (2) a settlement to be agreed and approved, are becoming clearer. In particular, the AFA and the PNF in France, and the SFO in the United Kingdom (in June and August 2019, respectively) have released guidance that clarifies their views on the co-operation needed to create the right conditions for a negotiated settlement to follow.[18] Courts and prosecutors have also provided guidance on whether corporate organisations are demonstrating the required levels of co-operation, while maintaining claims to legal professional privilege (where it is available).

16 'Regular compliance renewal helps French transport company minimise corruption fine', Global Investigations Review (2 August 2021), at https://globalinvestigationsreview.com/anti-corruption/regular-compliance-renewal-helps-french-transport-company-minimise-corruption-fine.

17 Department of Justice, 'Review Group Report on structures and strategies to prevent, investigate and penalise economic crime and corruption' (June 2021), at https://www.gov.ie/en/publication/be30e-review-group-report-on-structures-and-strategies-to-prevent-investigate-and-penalise-economic-crime-and-corruption/.

18 UK: see Serious Fraud Office, Corporate Co-operation Guidance, at https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/>. France: see French Anti-Corruption Agency, at https://www.agence-francaise-anticorruption.gouv.fr/files/files/Lignes%20directrices%20PNF%20CJIP.pdf; https://www.agence-francaise-anticorruption.gouv.fr/fr/lafa-et-parquet-national-financier-precisent-mise-en-oeuvre-convention-judiciaire-dinteret-public.

Culture and individual accountability

Among the most prominent themes in investigations concerning corporate organisations is the focus on culture, both at the time when alleged misconduct occurred and when any investigation is commenced. The definition of what constitutes 'good culture' is elusive. Authorities deciding whether to commence, continue and discontinue investigations (and selecting which charges to pursue) attach substantial importance to whether they consider alleged conduct (including individuals' conduct outside the workplace) to be indicative of a poor culture.

Although the FCA has historically published information about culture and governance as categories of enforcement data in their own right, it no longer does so. This perhaps suggests that the FCA views culture as pervasive across the firms that it regulates, and so it no longer needs to be explicitly identified as a stand-alone category.

The UK Senior Managers Certification Regime (SMCR) goes further than previous regulatory initiatives directed towards individual accountability. It gives the FCA and the Prudential Regulation Authority (PRA) powers to take action against a much broader population of individuals within firms. It also requires firms to document the specific responsibilities of their most senior executives, thus providing the FCA and PRA with clear road maps that may be used to hold those individuals accountable for breaches of regulatory requirements by firms. The FCA is now routinely using the SMCR for this purpose during enforcement investigations. Although enforcement authorities around Europe have been watching to see how the FCA and PRA seek to use these mechanisms to drive up standards of behaviour within the financial services industry, it remains to be seen whether other European regulators will follow the SMCR approach. By contrast, other common law jurisdictions, such as Singapore, Hong Kong and Australia,[19] have enacted regimes similar to the SMCR in recent years.

Even in countries where enforcement authorities have not explicitly named culture as an enforcement priority, boards are increasingly concerned to demonstrate their commitment to culture. Cases across Europe have shown the substantial reputational damage that can result from allegations of poor cultural practices and the speed at which allegations can cross borders (including into jurisdictions where enforcement authorities are active in this area).

Information sharing and multi-jurisdictional investigations

European investigation and enforcement authorities continue to collaborate actively with one another and with their counterparts globally, using mutual legal assistance treaties and other informal arrangements. There have been particularly noticeable increases in efforts to collaborate across borders where authorities have acquired the ability to enter into global settlements involving overseas enforcement authorities, and in GDPR-related enforcement.

Across Europe, traditional boundaries between enforcement authorities' remits are becoming increasingly blurred. The authorities are having to take an increasingly flexible

19 Singapore: Individual Accountability and Conduct Regime. Hong Kong: Manager-in-Charge Regime. Australia: Banking Executive Accountability Regime.

view of what they are responsible for investigating, which authority should take the lead and how they should most effectively collaborate. Overlaps between the remits of antitrust, data protection and financial services enforcement authorities are becoming increasingly apparent. One example of this flexibility was the close co-operation between Luxembourg's and France's data protection authorities when Amazon was investigated for violating the GDPR.[20]

Enforcement authorities, conscious of the potential for duplication and delay, are anticipating these overlaps, both within and between jurisdictions, and are implementing mechanisms to facilitate collaboration. For example, following Brexit, the FCA entered into a series of detailed memoranda of understanding with the relevant national competent authorities within the European Union and the European Economic Area, setting out how these agencies will co-operate and exchange information.[21] Although convictions and other enforcement outcomes in one jurisdiction will commonly be the product of extensive information sharing between authorities, there are as yet few significant concluded examples of enforcement authorities simultaneously pursuing enforcement cases against the same targets in multiple European jurisdictions.

EU institutions as enforcement authorities

Historically, there have been relatively few examples of supranational European authorities (other than the European Commission (EC) in its role as an antitrust enforcement authority) taking overarching enforcement action. That said, there is a clear movement to facilitate greater co-operation and coordination with respect to enforcement activity at a European level. This is both as a response to past incidents in which regulatory arrangements were found to have been lacking and in an effort to counter perceived growing threats.

In particular, the European Union has stepped up its focus on a pan-European approach to AML enforcement following AML failings in various European states. Until now, AML legislation encouraging closer collaboration between national investigation and enforcement authorities has taken the form of successive AML Directives (which, as they are not directly effective instruments and require transposition by Member States into their national laws, have been implemented in different ways and to different extents). For example as of May 2021:

- only 70 per cent of EU Member States had been identified as having fully transposed the fifth MLD into their national laws, despite a deadline of January 2020;[22] and

20 'The Luxembourg data protection authority fined Amazon Europe Core €746 million', National Commission for Computing and Liberty (3 August 2021), at https://www.cnil.fr/fr/lautorite-luxembourgeoise-de-protection-des-donnees-prononce-lencontre-damazon-europe-core-une.

21 'MoUs with European authorities in the areas of securities, investment services and asset management, insurance and pensions, and banking', Financial Conduct Authority (4 January 2021), at https://www.fca.org.uk/news/statements/mous-european-authorities-securities-insurance-pensions-banking.

22 'Anti-money laundering directive V (AMLD V) – transposition status', European Commission (2 June 2020), at https://ec.europa.eu/info/publications/anti-money-laundering-directive-5-transposition-status_en.

- the fourth MLD had yet to be completely transposed into the national laws of all EU Member States, despite 16 June 2017 being the deadline for doing so.[23]

The European Banking Authority (EBA) was given additional powers following several well-publicised AML failings. As of 1 January 2020, the EBA has been:

- tasked with coordinating national authorities' supervisory responsibilities in respect of AML activity;
- empowered to lead on the establishment of AML policies by national authorities; and
- required to monitor the implementation of AML standards within Europe.[24]

An example of the EBA's work in this area can be found in the revised guidelines on money laundering and terrorist financing risk factors published in March 2021. As part of a general update to the AML landscape in the European Union (EU AML), the guidelines address new money laundering risk factors and seek to develop more effective and consistent supervisory approaches across Europe.[25] It is apparent that the EBA will continue to rationalise the AML landscape. On 2 August 2021, the authority published a consultation paper[26] seeking views on draft guidelines setting out the role, tasks and responsibilities of AML compliance officers under the fourth MLD. It is the first time that the regulatory expectations for AML compliance officers have been set out at a European level, apparently with a view to adopting a similar EU-wide approach such as that required under the GDPR for data protection officers.

Despite this activity, arrangements are still far from uniform across Europe. The extent to which the requirements set out in successive MLDs have been effectively transposed, and other provisions relating to cross-border collaboration and resourcing of national authorities have been implemented, varies widely between jurisdictions and will require further action to resolve.

In some instances, bilateral and multinational arrangements are in place, helping authorities to deploy their resources as effectively and efficiently as possible in cross-border AML investigations. The most recent example, which is also a response to the concerns about previous enforcement arrangements already mentioned, is a formal mechanism to enable Baltic and Nordic AML regulators to exchange information and coordinate

23 'Anti-money laundering directive IV (AMLD IV) – transposition status', European Commission (5 October 2020), at https://ec.europa.eu/info/publications/anti-money-laundering-directive-4-transposition-status_en.

24 Regulation (EU) 2019/2175.

25 'EBA publishes final revised Guidelines on money laundering and terrorist financing risk factors', European Banking Authority [EBA] (1 March 2021), at https://www.eba.europa.eu/eba-publishes-final-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors.

26 Consultation Paper: Draft Guidelines: 'On policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849', EBA, at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Consultations/2021/Consultation%20on%20draft%20Guidelines%20on%20the%20role%2C%20tasks%20and%20responsibilities%20AML-CFT%20compliance%20officers/1018277/CP%20GLs%20on%20AMLCFT%20compliance%20officer.pdf.

enforcement action. There are also increasingly sophisticated mechanisms in place in some jurisdictions to enable information sharing between private sector organisations, and with enforcement authorities.[27] In July 2020, the Netherlands Bankers' Association announced that the country's three largest banks and two smaller lenders would create a purely private joint transaction monitoring body, called Transaction Monitoring Netherlands,[28] designed to flag activity of concern that would not necessarily be identified as suspicious by a single institution's compliance department. Transaction Monitoring Netherlands is due to begin monitoring transactions in 2021. However, at the time of writing, it was unclear whether it had.[29]

The EC also appears determined to take further action. On 20 July 2021, it unveiled a further package of legislative proposals to strengthen the EU AML framework. The package included the creation of a new EU enforcement agency tasked with combating money laundering, called the Anti-Money Laundering Authority (AMLA).[30] The intent is to establish AMLA as a 'centrepiece' of a supervisory system that includes national authorities. This will allow the EC to directly supervise certain high-risk entities and join the front-line of AML enforcement. This is a welcome development in light of recent AML scandals, which invariably involve a cross-border element, leaving national enforcement agencies piecing together an incomplete picture after the conduct has completed.

Away from AML enforcement, the EC remains active as an antitrust enforcement authority. Some long-standing themes continue to feature in European antitrust investigations. There are exceptions to rules relating to legal professional privilege (in jurisdictions where it is part of the legal landscape). Leniency provisions often do not dovetail neatly with other regulatory mandatory reporting obligations. There are significant variations in the approaches taken by the EC and national competition authorities. There would also appear to be a different focus on sectors of enforcement. The EC appears to be concentrating on technology companies, as opposed to perhaps the more traditional financial crime targets, namely financial institutions and extractive industries. These, and other themes, mean that European antitrust investigations have to be handled differently from those pursued by other regulators.

In other areas, authorities with a pan-European remit have been active. The European Anti-Fraud Office (known as OLAF), the division of the EC responsible for investigating fraud against the EU budget, and corruption and serious misconduct within EU institutions, has been particularly active in conducting investigations. The most recent available

27 In the United Kingdom, with effect from October 2017, previously voluntary arrangements enabling information sharing within the private sector and between private sector organisations and enforcement authorities were placed on a statutory footing – Criminal Finances Act 2017, s.11 (which amended the Proceeds of Crime Act 2002).

28 See press release, Netherlands Bankers' Association, 'Transaction Monitoring Netherlands: a unique step in the fight against money laundering and the financing of terrorism', at https://www.nvb.nl/english/transaction-monitoring-netherlands-a-unique-step-in-the-fight-against-money-laundering-and-the-financing-of-terrorism/.

29 See https://tmnl.nl/summary-eng/.

30 https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en.

statistics indicate that OLAF concluded 230 investigations and commenced 290 investigations during 2020 and recommended that national authorities take action to recover nearly €294 million in 2020.[31]

In addition, Europol has conducted extensive work to seek to coordinate national responses and lay the foundations for possible future multilateral criminal enforcement action in a number of areas, including notably in relation to large-scale cyberattacks[32] and the coronavirus pandemic.[33]

It seems likely that levels of coordinated pan-European criminal enforcement action will increase in future. The new European Public Prosecutor's Office (EPPO) became operational in June 2021. In the 22 Member States that have signed up to the arrangements establishing it,[34] EPPO will have powers to investigate and prosecute crimes against the EU budget, such as fraud, corruption and tax fraud valued at over €10 million. It will not replace OLAF or other existing investigating and prosecuting authorities (or national enforcement authorities) but will pool experience, adopt a consistent prosecution policy, and be able to use streamlined procedures for the exchange of information across borders. Laura Codruța Kövesi, the current head of EPPO and European Chief Prosecutor, has indicated a willingness to use EPPO's powers extensively.[35] Indeed, following a lengthy preparatory phase, EPPO started its investigations promptly, organising a coordinated series of searches in early August 2021 across five European jurisdictions in connection with a VAT fraud estimated to be worth €14 million.[36]

Brexit certainty?

Despite fears that Brexit would cause significant damage to cross-border investigations and enforcement, the December 2020 trade and co-operation deal (the Brexit Deal) did much to limit the consequences of Brexit in the areas of enforcement and investigations. In the context of the Irish border (a potential enforcement flashpoint), a UK parliamentary committee found (in April 2021) that 'Brexit had had no discernible operational

31 See European Anti-Fraud Office, 'The OLAF Report 2020', at https://ec.europa.eu/anti-fraud/system/files/2021-09/olaf_report_2020_en_0.pdf, p. 3.

32 See press release, Europol (30 June 2021), at https://www.europol.europa.eu/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups.

33 See press release, Europol (22 June 2021), https://www.europol.europa.eu/newsroom/news/terrorists-attempted-to-take-advantage-of-pandemic-says-europol%E2%80%99s-new-eu-terrorism-situation-and-trend-report-2021.

34 Sweden, Hungary, Denmark, Ireland and Poland having opted out.

35 See further details in relation to the European Public Prosecutor's Office at https://europa.eu/rapid/press-release_MEMO-17-1551_en.htm, and the appointment of the European Chief Prosecutor at www.europarl.europa.eu/news/en/press-room/20190923IPR61749/kovesi-to-become-eu-chief-prosecutor.

36 'Premises in Germany, the Netherlands, Slovakia, Bulgaria and Hungary searched in the framework of an EPPO investigation into cross-border VAT fraud' (4 August 2021), at https://www.eppo.europa.eu/en/news/premises-germany-netherlands-slovakia-bulgaria-and-hungary-searched-framework-eppo.

impact on cross-border policing and the ability to co-operate with partners in the EU has been maintained'.[37]

In addition to the Brexit Deal, the steps that the UK government took to maintain access to a similar level of information from European enforcement agencies following Brexit appear to be helping to maintain the status quo. In February 2021, the UK government stated that the Interpol systems and Warning Index used by the United Kingdom for law enforcement purposes, which are no longer automatically integrated into the UK Police National Computer following Brexit, update at broadly the same speed as the pre-Brexit systems.[38]

It should be noted, however, that Brexit is still only a recent development and that a greater impact may become apparent over time. It is likely that an assessment will only be possible once the backlog of pre-Brexit investigations and cases is resolved, and authorities begin to tackle post-Brexit investigations and cases. Areas of future concern include the European Investigation Order scheme and issues in replacing the European Arrest Warrant (EAW) scheme in the United Kingdom.

The United Kingdom is no longer part of the European Investigation Order scheme. The Brexit Deal provided that UK–EU arrangements would revert to a mutual legal assistance scheme governed by a 1959 convention. It would appear that the process of obtaining information under these new arrangements might take longer. Although the European Investigation Order scheme gave states 30 days from the receipt of a request to decide whether to execute it, the new arrangements allow 45 days.

Further, following its withdrawal from the EAW system, 10 EU Member States have notified the United Kingdom of their intention to exercise an absolute bar on the extradition of their own nationals to the United Kingdom, and an additional two nations shall only extradite their own nationals to the United Kingdom with the individual's consent.[39] It appears that the European and United Kingdom will need to take care to ensure cross-border enforcement action can be maintained, otherwise it is possible that the UK government will soon find it difficult to close cases against individuals of certain nationalities who have returned to their home nation in Europe. Before Brexit, the EAW would probably have resolved the issue. It remains to be seen whether this will prove to be a significant challenge for UK enforcement activity in the future.

37 'Cross-border co-operation on policing, security and criminal justice after Brexit', Northern Ireland Affairs Committee (22 April 2021), at https://committees.parliament.uk/publications/5650/documents/55754/default/.

38 National Crime Agency – Written evidence (PBS0001): Post EU Exit Law Enforcement Cooperation (3 February 2021), at https://committees.parliament.uk/writtenevidence/23533/pdf/.

39 Home Office – Written evidence (PBS0002): EU Member State Notifications under the Law Enforcement and Criminal Justice Title of the Trade and Cooperation Agreement, including Extradition Of Own Nationals (5 March 2021), at https://committees.parliament.uk/writtenevidence/23544/pdf/.

Appendix 1

About the Authors of Volume II

Robert Dalling

Jenner & Block London LLP

Robert Dalling is a partner in Jenner & Block's investigations, compliance and defence practice. Formerly a trial advocate with 10 years' courtroom experience, he has represented global financial institutions, multinational corporates and individuals in high-profile and high-value internal and external investigations involving a wide range of financial crime and other regulatory issues.

Rob has advised some of the world's largest financial institutions on financial sanctions, often in connection with complex and sophisticated financial products and transactions. He has experience in applying for licences from sanctions authorities in the United Kingdom. He advises companies on the development of internal policies (including on anti-bribery, anti-fraud, anti-money laundering and terrorist financing, conflicts of interest, gifts and hospitality, and supply chain and modern slavery issues) and associated procedures, controls and training. He has assisted several clients with complex anti-money laundering issues and has dealt with the National Crime Agency on a large number of consent applications.

Prior to moving into private practice, Rob spent several years practising as a barrister in white-collar criminal litigation. Market commentators for *Chambers and Partners* 2020 describe him as an 'excellent' lawyer who is 'incredibly clever and very tactical'.

Kelly Hagedorn

Jenner & Block London LLP

Kelly Hagedorn is a partner in both Jenner & Block's investigations, compliance and defence practice, and data privacy and cybersecurity practice. Kelly advises on white-collar crime matters, data protection and cybersecurity matters (including data breaches) and international disputes involving fraud allegations. She has particular expertise in matters involving the financial services, gaming, hospitality and outsourcing sectors.

In 2018, Kelly was named in *Global Data Review*'s inaugural '40 under 40' list of up-and-coming professionals working in the field of data law.

Matthew Worby

Jenner & Block London LLP

Matthew Worby is an associate in Jenner & Block's investigations, compliance and defence practice group. Matthew has experience of representing both international corporates in investigations and defending individuals against prosecution by the Serious Fraud Office.

Jenner & Block London LLP

Level 17, Tower 42
25 Old Broad Street
London, EC2N 1HQ
United Kingdom
Tel: +44 33 0060 5400
Fax: +44 33 0060 5499
khagedorn@jenner.com
rdalling@jenner.com
mworby@jenner.com
www.jenner.com

26

Fines, Disgorgement, Injunctions, Debarment: The US Perspective

Anthony S Barkow, Charles D Riely, Amanda L Azarian and Grace C Signorelli-Cassady[1]

26.1 Introduction

This chapter provides an overview of the potential fines, penalties and other collateral consequences that corporates and individuals may face in the United States under federal law when defending against, or settling an enforcement action with, US authorities. The chapter then provides examples of the fines, penalties and other remedies associated with particular federal criminal statutes of potential interest, including the Foreign Corrupt Practices Act and anti-money laundering statutes.

US enforcement authorities have a variety of means to seek redress from corporates and individuals, including financial penalties and equitable remedies. The general purpose and policy objectives behind these remedies are (1) to deter the defendant and others from committing such offences in the future, (2) to protect the public, (3) to punish the defendant and (4) to promote rehabilitation of the defendant.[2] In considering fines and penalties, the US enforcement authorities and courts will consider the facts and circumstances of the matter, including whether the defendant accepts responsibility for the conduct, any remediation that has been effected and co-operation by the defendant with the relevant enforcement authorities.[3]

See Chapter 10 on co-operating with authorities

1 Anthony S Barkow and Charles D Riely are partners, and Amanda L Azarian and Grace C Signorelli-Cassady are associates, at Jenner & Block LLP. The authors wish to acknowledge the contribution of Rita D Mitchell of Willkie Farr & Gallagher, the original author of the chapter in previous editions on which this chapter is partly based.

2 See, e.g., Department of Justice (DOJ), Justice Manual (Justice Manual) § 9-27.110.

3 See, e.g., Justice Manual § 9-27.420.

In recent years, both the Department of Justice (DOJ) and Securities and Exchange Commission (SEC) have been successful in extracting significant financial penalties as part of their enforcement actions and settlements. These penalties depend on the facts and circumstances and range from penalties in the five- to six-figure range[4] to settlements in the billions.[5] These include cases brought by the DOJ, individual US attorney offices and the SEC. For example, in the fiscal year ending in September 2020, the DOJ obtained more than US$2.2 billion in total settlements and judgments from civil cases brought pursuant to the False Claims Act alone.[6] Likewise, in 2020, the US Attorney's Office for the Eastern District of Virginia, which includes some of the area surrounding Washington, DC, collected more than US$242 million in criminal and civil actions.[7] The Southern District of New York announced two settlements in 2020, totalling nearly US$90 million between them alone.[8] In fiscal year 2020, the SEC brought 715 enforcement actions and obtained

4 See, e.g., DOJ press release, 'Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations' (31 May 2019), available at https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations; Department of Justice press release, 'Department Of Justice Reaches $5.5 Million Settlement With Van Andel Research Institute To Resolve Allegations Of Undisclosed Chinese Grants To Two Researchers' (19 Dec. 2019), available at https://www.justice.gov/usao-wdmi/pr/.

5 For example, in October 2020, the DOJ and SEC entered into the largest FCPA settlement to date with Goldman Sachs Group and its Malaysian subsidiary. The agencies imposed financial penalties totalling approximately US$3.3 billion to resolve charges in connection with a large-scale bribery scheme. (DOJ press release, 'Goldman Sachs Charged in Foreign Bribery Case and Agrees to Pay Over $2.9 Billion' (22 Oct. 2020), available at https://www.justice.gov/opa/pr/goldman-sachs-charged-foreign-bribery-case-and-agrees-pay-over-29-billion). Also in 2020, the SEC obtained a US$500 million penalty against Wells Fargo for misleading investors by opening 'authorized or fraudulent accounts for unknowing customers' (Securities and Exchange Commission, Division of Enforcement 2020 Annual Report, available at https://www.sec.gov/files/enforcement-annual-report-2020.pdf.).

6 DOJ press release, 'Justice Department Recovers Over $2.2 Billion from False Claims Act Cases in Fiscal Year 2020' (14 Jan. 2021), available at https://www.justice.gov/opa/pr/justice-department-recovers-over-22-billion-false-claims-act-cases-fiscal-year-2020.

7 DOJ press release, 'U.S. Attorney's Office in EDVA Recovers $242 Million in 2020 for Victims and in Criminal and Civil Matters' (8 Feb. 2021), available at https://www.justice.gov/usao-edva/pr/us-attorney-s-office-edva-recovers-242-million-2020-victims-and-criminal-and-civil.

8 DOJ press release, 'Acting Manhattan U.S. Attorney Announces $49 Million Settlement With Biotech Testing Company For Fraudulent Billing And Kickack Practices', (23 Jul. 2020), available at https://media.defense.gov/2020/Jul/28/2002465759/-1/-1/1/200723_ACTING%20MANHATTAN%20U.S.%20ATTORNEY%20ANNOUNCE._.PDF; DOJ press release, 'Acting Manhattan U.S. Attorney Announces $40.5 Million Settlement With Durable Medical Equipment Provider Apria Healthcare For Fraudulent Billing Practices', (21 Dec. 2020), available at https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-405-million-settlement-durable-medical-equipment.

judgments and orders totalling approximately US$4.68 billion in disgorgement and penalties – an SEC record.[9]

In 2018, the DOJ issued a policy emphasising the importance of prosecuting individuals and discouraging 'disproportionate enforcement of laws by multiple authorities'. The policy provided that prosecutors should 'avoid the unnecessary imposition of duplicative fines, penalties, and/or forfeiture' against a corporate being investigated by multiple enforcement authorities.[10] The policy requires DOJ lawyers from all departments to coordinate internally and, when possible, with 'other federal, state, local, or foreign enforcement authorities' to curb the practice of 'piling on' fines and penalties, 'with the goal of achieving an equitable result'.[11] Although it is difficult to measure the impact of these policies in practice, US authorities have continued to bring actions with multiple regulators and serious financial ramifications. Accordingly, corporates and individuals facing enforcement action should be mindful of the potential consequences and the opportunities to manage and reduce the ultimate fines and penalties.

26.2 Standard criminal fines and penalties available under federal law

26.2.1 Financial penalties

Many federal statutes contain their own fining provisions, which typically include a maximum fine amount. Additionally, for some crimes, the Alternative Fines Act provides for an alternative maximum fine of double the gross gain

9 Securities and Exchange Commission (SEC), Division of Enforcement 2020 Annual Report, available at https://www.sec.gov/files/enforcement-annual-report-2020.pdf.

10 Justice Manual § 1-12.100 – Coordination of Corporate Resolution Penalties in parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018).

11 The policy sets out various factors that should be considered when coordinating between multiple DOJ units or enforcement authorities, including 'the egregiousness of a company's misconduct; statutory mandates regarding penalties, fines, and/or forfeitures; the risk of unwarranted delay in achieving a final resolution; and the adequacy and timeliness of a company's disclosures and its cooperation with the Department, separate from any such disclosures and cooperation with other relevant enforcement authorities'. (Justice Manual § 1-12.100 – Coordination of Corporate Resolution Penalties in parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (May 2018).) An example of this policy in action can be found in the Department's March 2019 US$850 million settlement with MTS and related SEC settlement carrying a civil penalty of US$100 million. According to a press release: 'Consistent with Coordination of Corporate Resolution Penalties in Parallel and/or Joint Investigations and Proceedings Arising from the Same Misconduct (Justice Manual 1-12.100), the Department of Justice agreed to credit the civil penalty paid to the SEC as part of its agreement with MTS. Thus, the combined total amount of criminal and regulatory penalties paid by MTS and [its subsidiary] to U.S. authorities will be $850 million.' (DOJ press release, 'Mobile Telesystems Pjsc and Its Uzbek Subsidiary Enter Into Resolutions of $850 Million with the Department of Justice for Paying Bribes In Uzbekistan' (7 Mar. 2019), available at https://www.justice.gov/opa/pr/mobile-telesystems-pjsc-and-its-uzbek-subsidiary-enter-resolutions-850-million-department.)

(or gross loss caused to another) from the unlawful activity.[12] Where a fine is imposed against an officer, director, employee, agent or shareholder of a corporate issuer, the fine may not be paid, directly or indirectly, by the corporate issuer.[13]

For certain offences, the DOJ may also seek criminal or civil forfeiture, or both, of property that constitutes, or is derived from proceeds traceable to, the offence.[14] Recent examples of forfeiture include (1) nearly US$1.1 billion in assets recovered in connection with various forfeiture cases related to the international money laundering and bribery scheme involving the Malaysian sovereign wealth fund 1MDB,[15] and (2) more than US$54 million forfeited in 2020 related to the DC Solar Ponzi scheme where at least half of the solar generators claimed to have been manufactured by the defendant did not actually exist.[16]

Defendants may also be required to pay restitution, taking into consideration the amount of loss sustained by each victim, the financial resources of the defendant and any other factors the court deems appropriate.[17]

Although corporates may attempt to reduce the amount of financial fines or penalties by claiming an inability to pay, the DOJ closely scrutinises any such arguments. In October 2019, the DOJ issued a non-binding policy memorandum to Criminal Division attorneys that provides 'guidance and an analytical framework' on evaluating a company's ability to pay a criminal fine

12 See 18 U.S.C. § 3571; *Southern Union Co. v. United States*, 132 S.Ct. 2344, 2350-52 (2012).

13 15 U.S.C. § 78ff(c)(3).

14 See, e.g., 18 U.S.C. § 982(a) (in connection with sentencing persons convicted of certain federal offences, including money laundering and other financial crimes, courts shall order criminal forfeiture of property 'involved in such offense, or any property traceable to such property'); 18 U.S.C. § 981(a) (property involved in certain federal offences, including money laundering and other financial crimes, 'or any property traceable to such property', is subject to civil forfeiture). Under civil forfeiture statute 18 U.S.C. § 981(a)(1)(C), property relating to a 'specified unlawful activity' as defined in 18 U.S.C. § 1956(c)(7) is subject to civil forfeiture. Among the 'specified unlawful activities' listed in 18 U.S.C. § 1956(c)(7) are racketeering, bribery of a public official, fraud by or against a foreign bank, export control violations and violations of the FCPA. Further, 28 U.S.C. § 2461(c) 'permits the government to seek *criminal* forfeiture whenever civil forfeiture is available *and* the defendant is found guilty of the offense'. *United States v. Newman*, 659 F.3d 1235, 1239 (9th Cir. 2011) (original emphasis).

15 DOJ press release, 'United States Reaches Settlement to Recover More Than $49 Million Involving Malaysian Sovereign Wealth Fund' (6 May 2020), available at https://www.justice.gov/opa/pr/united-states-reaches-settlement-recover-more-49-million-involving-malaysian-sovereign-wealth.

16 DOJ press release, 'Court-Orders Final Forfeiture of Over $54 Million in Connection with Billion Dollar Ponzi Scheme' (15 April 2020), available at https://www.justice.gov/usao-edca/pr/court-orders-final-forfeiture-over-54-million-connection-billion-dollar-ponzi-scheme.

17 18 U.S.C. § 3663(a)(1)(B)(i).

or criminal monetary penalty when inability to pay is claimed.[18] The memo sets forth various legal considerations and relevant factors to take into account into account if legitimate questions remain after an analysis of an inability-to-pay questionnaire. These factors include background on current financial position, alternative sources of capital, collateral consequences and victim restitution considerations.

26.2.2 United States Sentencing Guidelines

Federal courts in the United States use the United States Sentencing Guidelines (the Sentencing Guidelines) as guidance in considering the aggravating and mitigating circumstances of a crime and imposing a sentence. These apply to both corporates and individuals. Although district courts must consult the Sentencing Guidelines, judges are not required to impose sentences – either prison terms or fines – within Guidelines ranges.[19] A recent study, in fact, suggests that federal trial judges 'now follow the advisory fraud guideline range in less than half of all cases', providing for sentences 'well below the fraud guideline'.[20]

For corporates, the calculation of the applicable fine under the Sentencing Guidelines is made by (1) identifying a 'base fine',[21] (2) identifying the minimum and maximum multipliers that combined with the base fine create a 'fine range'[22] and (3) considering whether any factors warrant any adjustments, upwards or downwards, to the fine range.[23]

In calculating the base fine under the Sentencing Guidelines, the first step is to identify the 'offence level', which depends on the characteristics of the crime. The 'base offence level' is set according to the nature of the conduct or the statute violated, and then the overall offence level will increase or decrease depending on certain factors.[24] For example, factors that may affect the overall offence level for a violation under the Foreign Corrupt Practices Act (FCPA) include the number of bribes, the amount involved and the position of the foreign official receiving the payment or benefit.[25] The total offence level helps to determine the

18 DOJ, Criminal Division, Memorandum on Evaluating a Business Organization's Inability to Pay a Criminal Fine or Criminal Monetary Penalty (8 October 2019), https://www.justice.gov/opa/speech/file/1207576/download.

19 The Sentencing Guidelines were mandatory until the Supreme Court's decision in *United States v. Booker*, 543 U.S. 220 (2005).

20 Mark Bennett, Justin Levinson and Koichi Hioki, 'Judging Federal White-Collar Fraud Sentencing: An Empirical Study Revealing the Need for Further Reform', *Iowa Law Review*, 989, Vol. 102:939 (2017); George Pierpoint, 'Is white-collar crime treated more leniently In the US?', BBC News (11 Mar. 2019), available at https://www.bbc.co.uk/news/world-us-canada-47477754.

21 United States Sentencing Commission, Guidelines Manual (Guidelines Manual), § 8C2.4.

22 Id., §§ 8C2.6, 8C2.7.

23 Id., §§ 8C4.1-8C4.11.

24 Base offence levels are set out in Chapter Two of the Guidelines Manual.

25 Guidelines Manual, §§ 2C1.1(b)(1)-(3).

base fine, which is the greatest of the amount specified in a table that translates the offence level into a base fine, the pecuniary gain to the organisation from the offence, or the pecuniary loss from the offence caused by the organisation, 'to the extent the loss was caused intentionally, knowingly, or recklessly'.[26]

The second step is to calculate the 'culpability score', which yields the minimum and maximum multipliers to be applied to the base fine. The culpability score is based on the characteristics of the defendant. Relevant factors may include the size of the organisation and the degree of participation in, or tolerance of, the wrongdoing; the defendant's prior criminal history; whether the defendant has violated an order or injunction, or violated a condition of probation by committing similar misconduct to that for which probation was ordered; obstruction of justice; the existence of an effective compliance programme; and self-reporting, co-operation and acceptance of responsibility.[27] The potential multipliers can range from 0.05 (a reduction of 20 times the base fine) to 4.0 (four times the base fine), depending on the culpability score. The fine range reflects the minimum and maximum multipliers as applied to the base fine. In addition to the fine, any gain to the corporate from an offence that is not otherwise part of the corporate's restitution or remediation is subject to disgorgement.[28]

Finally, the Sentencing Guidelines allow for adjustments from the fine range. This may include a reduction for substantial assistance to the government in its investigation of others[29] or remedial costs that exceed the gain to the corporate.[30] Unlike the factors that are considered for calculating the offence level and culpability score, the detriments or benefits that result from adjustments are not quantified. The court in its discretion imposes a fine within the fine range, or above or below the range. For negotiated resolutions, a corporate, through its counsel, will often negotiate the fine range with the government.

Civil penalties 26.3

Civil monetary remedies can include penalties, disgorgement and prejudgment interest. Each of these has a different purpose and method of calculation.

The SEC may impose civil monetary penalties on any person who violates or causes a violation of the securities laws. For example, the Securities Act of 1933 and the Securities Exchange Act of 1934 authorise three tiers of civil penalties, and the civil penalties imposed under these statutes can range from under US$10,000 to over US$1 million, per violation, after adjusting for inflation. Less serious civil violations fall into the first tier, where the penalty is no more than US$9,753 for an individual or US$97,523 for a corporate for

26 Id., § 8C2.4.

27 Id., § 8C2.5.

28 Id., § 8C2.9.

29 Id., § 8C4.1.

30 Id., § 8C4.9.

'each act or omission' violating the federal securities laws. The second tier applies to violations involving fraud, deceit, manipulation, or deliberate or reckless disregard of a regulatory requirement, for which the maximum penalty is US$97,523 for individuals and US$487,616 for corporates, again for each act or omission. Finally, the third tier applies to violations involving fraud, deceit, manipulation, or deliberate or reckless disregard of a regulatory requirement that also directly or indirectly resulted in 'substantial losses . . . to other persons' or 'substantial pecuniary gain to the person who committed the act or omission'.[31] Third-tier penalties have a limit of US$195,047 for individuals and US$975,230 for corporates, for each act or omission.[32] The SEC sometimes asserts that the defendant's conduct involved multiple violations and seeks a penalty for each violation. Therefore, in addition to determining the relevant tier, courts generally consider whether the conduct alleged constituted multiple violations. Civil penalties for insider trading depend on the amount of the profits generated by the illicit trading. A district court can order civil penalties up to three times the profit gained or loss avoided by the violative trade.[33]

The amount of penalties sought in resolved actions against corporates depends, in part, on how the SEC's leadership uses its discretion. A 2006 policy issued under the G W Bush administration, for example, emphasised the importance of avoiding further harm to shareholders by issuing penalties. Under its current leadership, though, the SEC is expected to aggressively seek penalties and emphasise deterrence. For example, Caroline Crenshaw, one of the current commissioners, delivered a speech in March where she criticised the SEC's historical approach to penalties as 'fundamentally flawed' and called for a reconsideration of the 2006 statement on penalties.[34] She argued that 'corporate penalties should be tied to the egregiousness of the actual misconduct – not just the benefit for impact on the shareholders' and claimed that her focus would be on 'vigorous enforcement of [the] existing laws and regulations' and 'ensuring that the violator pays the price'.[35] Crenshaw outlined other factors to be considered, including, self-reporting, co-operation, remediation, the extent of harm to the victim, pervasiveness or complicity within the organisation

31 15 U.S.C. § 78u-2(b); 17 C.F.R. § 201.1001 and SEC, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of 15 January 2021)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm (effective 15 January 2021). The maximum civil penalty amounts noted above are for violations after 2 November 2015. Maximum civil penalty amounts will be adjusted annually for inflation, as described in 17 C.F.R. § 201.1001.

32 Id.

33 15 U.S.C. § 78u-1(a).

34 SEC speech, Caroline Crenshaw, 'Moving Forward Together – Enforcement for Everyone' (9 Mar. 2021), available at https://www.sec.gov/news/speech/crenshaw-moving-forward-together.

35 Id. (emphasis removed).

and the difficulty of detecting the violations.[36] It is likely that a majority of commissioners echo Crenshaw's views and will follow these considerations when imposing penalties. [37]

The DOJ likewise may seek civil penalties in certain types of matters, such as violations of federal financial, health, safety, civil rights and environmental laws.[38] For example, in January 2021, Insitu Inc agreed to pay US$25 million to resolve allegations it violated the False Claims Act by knowingly submitting materially false cost and pricing data in relation to the supply of unmanned aerial vehicles to the military.[39]

Disgorgement and prejudgment interest 26.4

The SEC and the DOJ may also seek disgorgement to prevent an entity or individual from profiting from illegal conduct and to deter subsequent misconduct.[40] Disgorgement has often accounted for a significant portion of the overall enforcement sanction. For example, in July 2020, pharmaceutical company Alexion Pharmaceuticals Inc agreed to pay more than US$21 million to settle allegations that it had violated the FCPA, of which over US$14 million was disgorgement, as compared with approximately US$3.7 million in prejudgment interest and a US$3.5 million penalty.[41] Disgorgement can also be sought in certain circumstances even when the DOJ declines to prosecute the corporate under its Corporate Enforcement Policy. For example, in 2019, it declined

36 Id.

37 Soyoung Ho, 'Swift Change in SEC Enforcement Under Biden Administration', Thomson Reuters (11 Aug. 2021), available at https://tax.thomsonreuters.com/news/swift-change-in-sec-enforcement-under-biden-administration/.

38 See, e.g., 12 U.S.C. § 1833a (providing a civil money penalty provision to the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 which allows the DOJ to seek civil penalties against persons who violate one of 14 enumerated statutes); 42 U.S.C. § 3614(d)(1)(C) (allowing it to seek civil penalties for violations of the Fair Housing Act 1968).

39 DOJ press release, 'Insitu Inc. to Pay $25 Million to Settle False Claims Act Case Alleging Knowing Overcharges on Unmanned Aerial Vehicle Contracts' (12 Jan. 2021), available at https://www.justice.gov/opa/pr/insitu-inc-pay-25-million-settle-false-claims-act-case-alleging-knowing-overcharges-unmanned.

40 See *SEC v. Huffman*, 996 F.2d 800, 802 (5th Cir. 1993); *SEC v. Cavanaugh*, 445 F.3d 105, 117 (2d Cir. 2006) (noting that disgorgement 'has the effect of deterring subsequent fraud'); DOJ press release, 'Deutsche Bank Agrees to Pay over $130 Million to Resolve Foreign Corrupt Practices Act and Fraud Case' (8 Jan. 2021), available at https://www.justice.gov/opa/pr/deutsche-bank-agrees-pay-over-130-million-resolve-foreign-corrupt-practices-act-and-fraud (including US$681,480 in criminal disgorgement).

41 DOJ press release, 'Fresenius Medical Care Agrees to Pay $231 Million in Criminal Penalties and Disgorgement to Resolve Foreign Corrupt Practices Act Charges' (29 Mar. 2019), available at https://www.justice.gov/opa/pr/fresenius-medical-care-agrees-pay-231-million-criminal-penalties-and-disgorgement-resolve; SEC press release, 'SEC Charges Medical Device Company With FCPA Violations' (29 Mar. 2019), available at https://www.sec.gov/news/press-release/2019-48.

to prosecute Cognizant Technology Solutions for violations of the FCPA, yet the company agreed to pay nearly US$20 million in disgorgement, which represented 'all profits fairly attributable to the bribery conduct'.[42]

In 2021, Congress made several important changes to the US securities laws that will impact the SEC's ability to recover funds though disgorgement. Specifically, Congress passed a provision titled 'Investigations and Prosecution of Offenses for Violations of the Securities Laws'.[43] This provision amended certain disgorgement-related provisions of the Securities Exchange Act of 1934 to (1) expressly grant the SEC statutory authority to pursue disgorgement as a remedy for civil enforcement actions in federal court, (2) extend the statute of limitations for all disgorgement actions involving fraud and scienter from five years to 10 years, and (3) direct courts to apply a 10-year statute of limitations for all other claims seeking equitable remedies, such as injunctions, bars, suspensions, and cease and desist orders. Therefore, with this legislation, Congress has greatly expanded the time frame in which the SEC can seek disgorgement, also increasing the total disgorgement the SEC can collect.

This legislation was perceived by many to be a reaction to the US Supreme Court's recent decisions in *Kokesh* and *Liu*. In *Kokesh v. SEC*, the US Supreme Court had held in 2017 that the SEC's disgorgement remedy was subject to a strict five-year statute of limitations, explaining that '[d]isgorgement in the securities-enforcement context is a "penalty" . . . and so disgorgement actions must be commenced within five years of the date the claim accrues'.[44] Following the US Supreme Court's ruling in *Kokesh*, this statute of limitations had significantly impacted the SEC's ability to obtain disgorgement. Indeed, in its 2019 annual report, the SEC estimated that the Kokesh ruling had 'caused the [SEC] to forgo approximately $1.1 billion in disgorgement in filed cases'.[45]

The new legislation also addressed, at least in part, potential limitations to the SEC's disgorgement powers from a June 2020 Supreme Court case, *Liu v. SEC*. There, the Court held that the SEC could continue to seek disgorgement pursuant to its power to award 'equitable relief' under Section 21(d)(5) of the Securities Exchange Act but also held that the SEC could only do so where the disgorgement sought does not exceed the defendant's net profits and is awarded for victims. In doing so, the majority, without reaching any conclusions, also raised the possibility that disgorgement awards may not be an equitable remedy – and therefore not allowed under the relevant statute – in situations where courts decline to deduct expenses from the award, impose joint-and-several liability or fail to return money to investors. With its

42 DOJ Declination Letter, 'Re: Cognizant Technology Solutions Corporation' (13 Feb. 2019), available at https://www.justice.gov/criminal-fraud/file/1132666/download.

43 William M (Mac) Thornberry, National Defense Authorization Act for Fiscal Year 2021, available at https://www.congress.gov/bill/116th-congress/house-bill/6395/text?r=8&s=1.

44 *Kokesh v. SEC*, 137 S.Ct. 1635, 1639 (2017).

45 SEC, Division of Enforcement Annual Report (2019), available at https://www.sec.gov/files/enforcement-annual-report-2019.pdf.

legislation, though, Congress confirmed the SEC's ability to obtain disgorgement even where money is not distributed to investors. However, notwithstanding the 2021 legislation, some of the residual questions in *Liu* remain unresolved, meaning open questions related to the SEC's enforcement abilities will continue to be addressed by courts.

Beyond disgorgement, the SEC also generally obtains prejudgment interest on any disgorgement amount. The rules that apply to administrative proceedings brought by the SEC require that such amounts be included in any disgorgement.[46] District courts presiding over actions generally may determine whether prejudgment interest is appropriate.[47] The interest rate applied is typically the 'underpayment' rate set by the IRS.[48] There is no single approach for measuring when the clock begins to run on interest calculations. In some cases, it has been measured from the date the ill-gotten funds were received, up to the date of judgment.[49] In others, it may run from multiple dates where the matter involves multiple transactions,[50] or, where the applicable dates are difficult to identify, from the date of the complaint.[51]

Injunctions 26.5

The DOJ may also seek affirmative relief through an injunction where it is deemed necessary to advance public interests or enforce government functions. Such injunction actions may be specifically provided for by statute, may be used to enforce statutes that do not specifically provide for injunctive relief or may be sought from an appellate court pursuant to the All Writs Act.[52]

Likewise, the SEC may seek either a preliminary or permanent injunction when it appears that a person is engaged in, or is about to engage in, acts

46 17 C.F.R. § 201.600(a).

47 *SEC v. First Jersey Sec., Inc.*, 101 F.3d 1450, 1476 (2d Cir. 1996).

48 Id., 101 F.3d at 1476 (citing SEC Rules and Regulations, 60 Fed. Reg. 32738, 32788 (23 Jun. 1995)). See also 17 C.F.R. § 201.600(b). The underpayment rate charged by the IRS is three percentage points above the federal short-term rate and for purposes of calculating interest on sums disgorged is compounded quarterly. 26 U.S.C. § 6621(a)(2); 17 C.F.R. § 201.600(b).

49 *SEC v. DiBella*, 2008 WL 6965807 at *3 (D. Conn. 18 July 2008); *SEC v. GMC Holding Corp.*, 2009 WL 506872 at *6 (M.D. Fla. 27 Feb. 2009) ('The time frame for the imposition of prejudgment interest usually begins with the date of the unlawful gain and ends at the entry of judgment.') (quoting *SEC v. Yun*, 148 F. Supp. 2d 1287, 1293 (M.D. Fla. 2001).

50 S*EC v. Savino*, 2006 WL 375074 at *18 & n.10 (S.D.N.Y. 16 Feb. 2006) (calculating interest from the first day of the month following each improper trade).

51 *SEC v. United Energy Partners, Inc.*, 2003 WL 223392 at *2 n.12 (N.D. Tex. 28 Jan. 2003), aff'd, 88 F. App'x 744 (5th Cir. 2004) (using date of complaint for accrual of prejudgment interest award where dates on which defendant acquired disgorged funds were not clear); *SEC v. GMC Holding Corp.*, 2009 WL 506872 at *6 (M.D. Fla. 27 Feb. 2009) (same).

52 28 U.S.C. § 1651(a). See US Department of Justice Civil Resource Manual, 'Injunctions', available at https://www.justice.gov/jm/civil-resource-manual-214-injunctions.

or practices constituting a violation of the securities laws.[53] For example, in March 2020, the SEC obtained a preliminary injunction barring the company Telegram from delivering digital tokens called Grams, after the court held that the SEC had shown there was a sufficient likelihood that Telegram's sales were part of a larger scheme to unlawfully distribute the Grams.[54]

26.6 Other consequences

In addition to the criminal and civil penalties noted above, defendants may face other consequences as a result of a US criminal or civil action. For one, defendants may also face civil and criminal forfeiture of assets, including real and personal property constituting, or derived from proceeds traceable to, a violation, or to a conspiracy to commit a violation.[55] For certain offences, courts are required to order that property traceable to an offence be forfeited.[56]

See Chapters 18 on individuals in cross-border proceedings and 31 on individual penalties

Further, investigation or prosecution by authorities in one jurisdiction may also lead to investigations, prosecutions or resolution short of prosecution by authorities in other jurisdictions. For example, in January 2020, the largest foreign bribery settlement to date was entered into between airplane manufacturer Airbus and authorities in France, the United Kingdom and the United States. Airbus agreed to pay combined penalties of over US$3.9 billion to resolve anti-corruption and export control violations.[57] It is expected that this trend of multinational investigations and co-operation across jurisdictions will continue in the coming years.

See Chapter 24 on negotiating global settlements

Defendants may also face a variety of actions from other US government agencies, international organisations, other corporates or even shareholders and employees, actions which may involve additional litigation and other monetary penalties or debarment. These 'tag along' actions can even arise from investigations of unrelated conduct that are assisted by co-operation clauses required by prior settlements.[58]

---

53 15 U.S.C. § 77t(b); 15 U.S.C. § 78u(d).

54 SEC press release, 'Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges' (26 Jun. 2020), available at https://www.sec.gov/news/press-release/2020-146.

55 See 18 U.S.C. §§ 981, 982; 28 U.S.C. § 2461.

56 See 18 U.S.C. § 982. Examples of offences where forfeiture is required include, but are not limited to, laundering of monetary instruments under 18 U.S.C. § 1956, engaging in monetary transactions derived from specified unlawful activity under 18 U.S.C. § 1957, receipt of commissions or gifts for procuring loans under 18 U.S.C. § 215 and fraud by wire, radio, or television under 18 U.S.C. § 1343.

57 See DOJ press release, 'Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case' (31 Jan. 2020), available at https://www.justice.gov/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.

58 For example, in 2016, Odebrecht entered into a plea agreement with the DOJ for FCPA violations requiring it to co-operate fully with investigations conducted by multilateral development banks. On 29 January 2019, the World Bank debarred Odebrecht SA's

In addition, in connection with certain types of enforcement actions, such as FCPA enforcement, money laundering and sanctions violations, corporates may also be required to retain corporate compliance monitors. For example, in May 2021, State Street Corporation entered into a two-year deferred-prosecution agreement pursuant to which it agreed not only to pay a US$115 million criminal penalty but also to retain an independent corporate compliance monitor for two years.[59]

See Chapter 33 on monitorships

Finally, in some circumstances, individuals or entities may be barred or suspended from doing business with the executive branch of the United States government.[60] Debarment may be triggered by a criminal conviction or, in some circumstances, even an adverse civil judgment, and applies to all subdivisions of a corporation unless the decision is limited by its terms to specific divisions or organisational units.[61] Suspension may occur upon adequate evidence that certain wrongdoing was committed and when it is in the public's interest.[62] Like debarment, suspension affects all organisational divisions of a corporation, unless otherwise specified.[63]

Remedies under specific statutes 26.7

By way of example, the fines, penalties and other remedies associated with particular federal criminal statutes of potential interest are outlined below.

Foreign Corrupt Practices Act 26.7.1

The FCPA criminalises bribery of foreign officials, either directly or through an intermediary, to obtain business or some other benefit. Its anti-bribery provisions apply not only to all US corporates and persons, but also can apply to foreign corporates that issue securities within the United States or file certain reports with the SEC (issuers) and to these issuers' officers and employees, among others. The FCPA also criminalises actions taken in the United States by foreign corporates or their agents that are in furtherance of an improper

Brazilian construction and engineering subsidiary for three years, crediting '[d]isclosures from prior settlements' as contributing to the World Bank's investigation. Plea Agreement, United States District Court E. Dist. of NY against Odebrecht S.A., Cr. No. 16-643 (RJD) (21 Dec. 2016), at 11, available at https://www.justice.gov/opa/press-release/file/919916/download; World Bank Group Sanctions System Annual Report FY19, at 20, available at http://documents1.worldbank.org/curated/en/980641572096094561/pdf/World-Bank-Group-Sanctions-System-Annual-Report-FY19.pdf.

59 See DOJ press release, 'State Street Corporation to Pay $115 Million Criminal Penalty and Enter Into Deferred Prosecution Agreement in Connection With Scheme to Overcharge Custody Customers' (13 May 2021), available at https://www.justice.gov/usao-ma/pr/state-street-corporation-pay-115-million-criminal-penalty-and-enter-deferred-prosecution.

60 48 C.F.R. §§ 9.406-1(c), 9.407-1(d).

61 48 C.F.R. §§ 9.406-1(b), 9.406-2(a).

62 48 C.F.R. §§ 9.407-1(a), 9.407-2(a).

63 48 C.F.R. § 9.407-1(c).

payment or offer. Further, the FCPA's books and records and internal controls provisions also require corporates whose securities are listed in the United States or who file reports with the SEC to keep accounting records that accurately reflect the corporate's transactions and to maintain a system of internal controls.[64]

Violations of the FCPA can result in heavy penalties. For one, corporate entities may be subject to financial penalties of up to US$2 million per violation of the FCPA's anti-bribery provisions,[65] US$25 million per violation of the FCPA's accounting provisions,[66] or up to twice the gross pecuniary gain or loss from the violation pursuant to the Alternative Fines Act.[67] In addition, civil penalties for FCPA anti-bribery and accounting provisions violations may apply.[68]

Further, certain individuals may be either fined up to US$100,000 (US$250,000 under the Alternative Fines Act or twice the gain or loss from the violation) or imprisoned for up to five years, or both, for a criminal violation of the FCPA's anti-bribery provisions.[69] For criminal violations of the FCPA's accounting provisions, certain individuals can be subject to a fine of up to US$5 million or imprisonment for up to 20 years, or both.[70] Individuals may also face civil penalties for FCPA anti-bribery and accounting provisions violations.[71] Issuers, as defined under the FCPA, are prohibited from paying these individuals' criminal and civil fines.[72]

Moreover, the DOJ may also bring a civil action to seek an injunction against domestic concerns and persons other than issuers to prevent a current or imminent FCPA violation.[73] Likewise, the SEC may seek injunctions to prevent FCPA violations from occurring.[74]

In addition, disgorgement is often a key component of a civil FCPA esolution. For example, in October 2020, Goldman Sachs agreed to pay the DOJ and SEC more than US$2.9 million to resolve FCPA charges related to the

64 15 U.S.C. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a), 78(m).

65 15 U.S.C. §§ 78dd-2(g)(1)(A), 78 dd-3(e)(1)(A), 78ff(c)(1)(A).

66 15 U.S.C. § 78ff(a).

67 18 U.S.C. § 3571 (c)(2), (d).

68 15 U.S.C. §§ 78ff(c)(1)(B), 78u(d)(3); 17 C.F.R. § 201.1001; SEC, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of January 15, 2019)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm.

69 15 U.S.C. §§ 78dd-2(g)(2), 78dd-3(e)(2); 18 U.S.C. § 3571 (b)(2), (b)(3), (d).

70 15 U.S.C. § 78ff(a).

71 15 U.S.C. §§ 78ff(c)(2)(B), 78u(d)(3); 17 C.F.R. § 201.1001; SEC, 'Inflation Adjustments to the Civil Monetary Penalties Administered by the Securities and Exchange Commission (as of January 15, 2019)', available at https://www.sec.gov/enforce/civil-penalties-inflation-adjustments.htm.

72 15 U.S.C. § 78ff(c)(3).

73 15 U.S.C. §§ 78dd-2(d), 78dd-3(d).

74 15 U.S.C. § 78u(d)(1).

1MDB bribery scheme. Of the total amount paid by Goldman Sachs to settle the SEC charges (more than US$1 billion), US$606.3 million was disgorgement.[75] However, as discussed above in detail, the SEC's use of disgorgement in civil actions has been limited by the Supreme Court's decision in *Liu v. SEC*.[76]

For corporates seeking to avoid the heaviest penalties, however, the FCPA Corporate Enforcement Policy establishes a presumption that, 'absent aggravating circumstances' such as involvement by executive management in the misconduct or significant profit to the corporate from the misconduct, a corporate will receive a declination if it 'has voluntarily self-disclosed misconduct in an FCPA matter, fully cooperated, and timely and appropriately remediated'. Moreover, even if aggravating circumstances are present, for a corporate that voluntarily self-discloses, fully co-operates and timely and appropriately remediates, the DOJ will still recommend a 50 per cent reduction off the low end of the US Sentencing Guidelines fine range, except in the case of a recidivist.[77]

On 20 November 2019, the FCPA Corporate Enforcement Policy was amended to clarify that a corporate that voluntarily discloses misconduct need not disclose 'all relevant facts known to it', but simply 'all relevant facts known to it at the time of the disclosure'. In addition, the new policy explains that, for a corporate to fully co-operate, it must identify 'relevant evidence not in the company's possession' that the corporate is aware of.[78] However, the corporate is no longer required to identify opportunities 'to obtain relevant evidence not in the company's possession and not otherwise known to the Department' that the corporate 'is or should be aware of'.[79]

Federal criminal money laundering 26.7.2

The principal federal criminal money laundering statutes are 18 USC Sections 1956 and 1957. Section 1956 generally prohibits a person from knowingly engaging in financial transactions with the proceeds of certain unlawful activities to promote further unlawful activity, concealing the proceeds, evading taxes or avoiding reporting requirements. Section 1957 also prohibits a person from knowingly engaging in a monetary transaction involving property valued at more than US$10,000 that derives from specified unlawful activities. In regard

75 SEC press release, 'SEC Charges Goldman Sachs With FCPA Violations' (22 Oct. 2020), available at https://www.sec.gov/news/press-release/2020-265.

76 *Liu v. SEC*, No. 18-1501, 2020 WL 3405845, (U.S. 22 Jun. 2020).

77 DOJ, FCPA Corporate Enforcement Policy, available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

78 Id. On 3 July 2020, the DOJ and the SEC issued the first comprehensive update to the FCPA Resource Guide since it was first published in 2012, which now includes a section on the FCPA Corporate Enforcement Policy. A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition, at 51 (Jul. 2020), available at https://www.justice.gov/criminal-fraud/file/1292051/download.

79 DOJ, FCPA Corporate Enforcement Policy (updated March 2019), available at https://www.justice.gov/criminal-fraud/file/838416/download.

to both sections, the specified unlawful activities include proceeds resulting from offences involving bribery of a foreign official, fraud by or against a foreign bank, and certain smuggling and export control violations, to name a few.[80]

See Chapters 18 on individuals in cross-border proceedings and 31 on individual penalties

Any violation of Section 1956 is punishable by imprisonment for not more than 20 years, a fine of up to US$500,000 or twice the value of the property involved, or both. In addition, such violations can incur a civil penalty up to the greater of US$10,000 or the value of the property involved in the offence, plus asset forfeiture. For Section 1957, the maximum penalty is 10 years' imprisonment or a fine of up to twice the value of the property involved, or both.[81]

26.7.3 Export controls and trade sanctions

The US Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces most US economic sanctions. However, the US Commerce Department's Bureau of Industry and Security and DOJ National Security Division also enforce some aspects of US sanctions. Generally, these sanctions, such as the blocking of assets and trade restrictions, are used to accomplish national security and foreign policy objectives.

The sanctions can be either comprehensive for a jurisdiction, such as Cuba,[82] or targeted to particular individuals and entities, such as the sanctions imposed on one Chinese government entity and specific officials pursuant to the global Magnitsky Human Rights Accountability Act.[83] Typically, US sanctions either restrict activities that take place in the US or restrict activities that involve a 'US person', generally defined widely to include US citizens, permanent residents, persons present in the United States, and corporates organised under the laws of the United States or any jurisdiction therein, as well as those corporates' foreign branches.[84] However, non-US persons and corporates can face penalties under US sanctions as well, including for 'causing' a violation by a US person.[85] For example, in 2019, OFAC entered into a settlement with British Arab Commercial Bank plc, a UK-based commercial bank, in part for causing US financial institutions to engage in prohibited conduct involving Sudan.[86]

Fines for violations of the sanctions regulations can be significant. As of 18 August 2021, OFAC had settled 11 enforcement actions, with civil penalties

80 18 U.S.C. §§ 1956, 1957.

81 Id.

82 Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 83 Fed. Reg. 46347 (10 Sep. 2018).

83 Department of the Treasury, 'Treasury Targets Iranian-Backed Hizballah Officials for Exploiting Lebanon's Political and Financial System' (9 Jul. 2019), available at https://home.treasury.gov/news/press-releases/sm724.

84 See, e.g., 31 C.F.R. §§ 560.312, 560.314.

85 See, e.g., 50 U.S.C. § 1705(a).

86 Department of the Treasury, 'Settlement Agreement' (Jul. 2017), available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/transtel_settlement.pdf.

totalling more than US$15 million in 2021.[87] And in 2020, it settled 16 enforcement actions for just over US$23.5 million.[88] Criminal penalties for wilful violations of OFAC sanctions can include fines ranging up to US$1 million per violation or imprisonment of up to 20 years, or both.[89] Under Title 18, Section 3571, the government can also pursue fines and penalties against an organisation of up to US$500,000 or twice the pecuniary gain or loss derived from the offence, as well as forfeiture under 18 USC Section 981. Further, penalties for violations of the Trading with the Enemy Act, which provides the statutory authority for the Cuba sanctions, can be up to US$90,743 per violation (which may be adjusted for inflation), and criminal penalties can reach US$1 million.[90] Financial penalties for violations of the International Emergency Economic Powers Act, which underlies other sanctions programmes, are also possible; associated civil penalties can be up to US$250,000 or twice the amount of the unlawful transaction, and criminal penalties permit a fine of up to US$1 million and imprisonment of up to 20 years.[91]

See Chapter 45 on sanctions

Racketeer Influenced and Corrupt Organizations Act 26.7.4

The Racketeer Influenced and Corrupt Organizations Act (RICO) provides criminal penalties as well as a civil, private cause of action for acts performed as part of a criminal organisation or enterprise.[92] The statute contains variations on the proscribed conduct but generally criminalises participation in an 'enterprise' in interstate or foreign commerce through a 'pattern of racketeering

87 Department of the Treasury, '2021 Enforcement Information', available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information.

88 Department of the Treasury, '2020 Enforcement Information', available at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information/2020-enforcement-information.

89 See, e.g., 50 U.S.C. § 1705(c).

90 31 C.F.R. § 501.701; Continuation of the Exercise of Certain Authorities Under the Trading With the Enemy Act, 83 Fed. Reg. 46347 (10 Sep. 2018) (extending the expiration of Cuba sanctions pursuant to the Trading with the Enemy Act until September 2019).

91 50 U.S.C. § 1705; 31 C.F.R. § 501; Congressional Research Service, 'The International Emergency Economic Powers Act: Origins, Evolution, and Use' (20 Mar. 2019), available at https://fas.org/sgp/crs/natsec/R45618.pdf.

92 18 U.S.C. §§ 1961, et seq.

activity'.[93] Such racketeering activity includes mail and wire fraud and money laundering violations under Sections 1956 and 1957, as outlined above.[94]

RICO violations are punishable by fines and imprisonment for up to 20 years, plus forfeiture of any interest acquired or maintained through the violation, any interest in any enterprise that was established, operated, controlled, conducted or participated in as part of the RICO violation (or the property of such an enterprise) and any property constituting or derived from any proceeds that the person obtained, directly or indirectly, from racketeering activity.[95]

Additionally, the government may seek pre-indictment restraining orders for the purpose of preventing defendants from transferring assets the government may potentially seek to have forfeited. To obtain such an order, the government must establish that (1) there is a substantial probability that it will prevail on the forfeiture issue, (2) property will be destroyed or placed beyond the court's reach without the order and (3) the need to maintain the property's availability outweighs the hardship of a restraining order. Pre-indictment restraining orders are effective for 90 days, but can be extended for good cause or as a result of the filing of an information or indictment.[96]

There are also civil remedies under RICO available to any person injured by a RICO defendant, which include treble damages sustained by the injured party and the cost of the lawsuit, including reasonable attorneys' fees.[97]

26.8 Conclusion

Corporates and individuals may face a variety of fines, penalties and other collateral consequences when defending against or settling an enforcement action with US authorities. As has been explained, these risks can be substantial. That said, these risks can be managed, mitigated or avoided by engaging knowledgeable external counsel, who can evaluate the situation, provide advice and thereby enable the corporate or individual to make an informed decision about how to proceed.

93 18 U.S.C. § 1962. The first variation makes it unlawful for any person who has received any income derived from a pattern of racketeering activity to use any part of such income or its proceeds to acquire, establish or operate any enterprise involved in interstate or foreign commerce. 18 U.S.C. § 1962(a). The second variation makes it unlawful for any person to engage in a pattern of racketeering activity to acquire or maintain any interest in any enterprise involved in interstate or foreign commerce. 18 U.S.C. § 1962(b). The third variation makes it unlawful for any person employed by or associated with any enterprise involved in interstate or foreign commerce to conduct the enterprise's affairs through a pattern of racketeering activity. 18 U.S.C. § 1962(c). The statute also makes it unlawful for a person to conspire to participate in the conduct outlined in (a), (b) or (c). 18 U.S.C. § 1962(d).

94 18 U.S.C. § 1961(1).

95 18 U.S.C. § 1963(a).

96 18 U.S.C. § 1963(d).

97 18 U.S.C. § 1964(c).

Appendix 1

About the Authors of Volume I

Anthony S Barkow
Jenner & Block LLP

Anthony Barkow is co-chair of Jenner & Block's investigations, compliance and defence practice, and a member of the firm's markets and trading and government controversies practices. He represents companies and executives in global and national criminal and regulatory investigations. He also conducts internal investigations for corporations and other institutions, provides counsel to senior management on enforcement and compliance issues, and serves as a corporate monitor. As a federal prosecutor for 12 years in the United States Attorney's Offices for the Southern District of New York and the District of Columbia, and in Main Justice, he prosecuted some of the most significant international terrorism and white-collar criminal cases in the country. He has tried over 40 cases and briefed and argued more than 10 cases on appeal. During his government service, Mr Barkow was awarded the Attorney General's Award for Exceptional Service, the highest award bestowed by the Attorney General in the Department of Justice. He graduated from Harvard Law School, where he was Notes Office co-chair and supervising editor of the *Harvard Law Review*, and the University of Michigan.

Charles D Riely
Jenner & Block LLP

Charles Riely is a partner at Jenner & Block and a member of its investigations, compliance and defence, markets and trading and securities litigation and enforcement practices. Before joining Jenner & Block, he served as a lawyer at the Securities and Exchange Commission (SEC) for more than a decade, most recently as assistant regional director for the SEC's Division of Enforcement. While with the SEC, he worked on matters involving disclosure failures by public companies, alleged fraud and regulatory violations by investment advisers and broker-dealers, insider trading, anti-money laundering violations, 'spoofing' and other forms of market manipulation, failure-to-supervise violations,

the adequacy of firms' cybersecurity procedures and protections, and a variety of other fraud and regulatory matters. Mr Riely also coordinated investigations with the US Department of Justice and worked on more than a dozen publicly filed SEC enforcement actions in which criminal authorities filed a parallel case. He graduated from the University of Michigan Law School and served as a law clerk to the Hon Frank Maas of the US District Court for the Southern District of New York. He is admitted to practise in New York.

Amanda L Azarian

Jenner & Block LLP

Amanda Azarian is an associate at Jenner & Block's London office focusing on investigations, compliance and defence. Ms Azarian has extensive experience in working on a range of government enforcement actions in the United States and United Kingdom, including large, complex matters involving the SFO, NCA, DOJ, SEC and OFAC, with a concentration on economic crime. Her practice includes the representation of both corporates and individuals, conducting and advising on global internal investigations, defending against allegations relating to financial crime and responding to government requests, offering compliance advice including in relation to anti-bribery and corruption, anti-money laundering, and sanctions and developing and implementing tailored compliance programmes, due diligence and risk assessments. Prior to joining Jenner & Block, Ms Azarian worked for the Washington, DC and London offices of an international law firm. Ms Azarian received her law degree from the Catholic University of America, Columbus School of Law, where she served as a staff member of the Catholic University Law Review and interned for the Hon Heidi Pasichow at the Superior Court for the District of Columbia. She is admitted to practise in both Maryland and Washington, DC.

Grace C Signorelli-Cassady

Jenner & Block LLP

Grace Signorelli-Cassady is an associate at Jenner & Block focusing on investigations, compliance and defence. Her experience includes assisting corporates in responding to government enquiries, including by US and European enforcement authorities; assisting corporates in conducting complex, worldwide internal investigations, including in connection with allegations of money laundering, bribery and corruption; and representing criminal defendants at trial and post-conviction, including individuals in white-collar matters, including for misrepresentations to investors and mail and wire fraud. She has also drafted nearly a dozen *amicus curiae* briefs regarding white-collar and criminal law issues, most of which were filed with the US Supreme Court. Prior to joining Jenner & Block, Ms Signorelli-Cassady served as a law clerk to the Hon Roslyn O Silver of the US District Court for the District of Arizona, during which time she assisted with matters taken by designation in the US Court of Appeals for the Ninth Circuit. Ms Signorelli-Cassady received her law degree from Harvard Law School, where she was the managing editor of the *Harvard Journal on Legislation*, selected as a criminal justice fellow and trained in negotiation techniques. She is admitted to practise in Illinois.

Jenner & Block LLP

Jenner & Block London LLP
25 Old Broad Street
London, EC2N 1HQ_
United Kingdom
Tel: +44 330 060 5400
Fax: +44 330 060 5499
aazarian@jenner.com

353 N Clark Street
Chicago, IL 60654-3456
United States
Tel: +1 312 222 9350
criely@jenner.com
gsignorelli@jenner.com

919 Third Avenue
New York, NY 10022-3908
United States
Tel: +1 212 891 1600
abarkow@jenner.com

www.jenner.com

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-272-5