CorporateLiveWire

FRAUD & WHITE COLLAR CRIME 2021

VIRTUAL ROUND TABLE

www.corporatelivewire.com

Introduction & Contents

This roundtable discusses the key fraud & white collar crime implications regarding COVID-19, the shift towards remote working, and Brexit. It also outlines best practice advice on a wide range of key topics such as what steps to take upon discovering fraud, effectively managing cross-border investigations, and corporate governance and internal control considerations. Featured jurisdictions are: Asia-Pacific, European Union, Japan, United Kingdom, and the United States.

James Drakeford
Editor In Chief

6 Q1. Have there been any recent regulatory changes or interesting developments?

9 Q2. Are there any compliance issues or potential pitfalls that firms need to be cautious about?

12 Q3. Have there been any noteworthy case studies or examples of new case law precedent?

15 Q4. How has COVID-19 impacted the fraud & white collar crime landscape?

18 Q5. What new challenges have emerged as a result of the shift towards remote working and what steps should companies take to remediate these risks?

19 Q6. Can you outline the best practice for corporate governance and internal control considerations?

22 Q7. What steps should a company should take upon discovering fraud?

25 Q8. What advice would you give to clients involved in cross-border investigations?

29 Q9. What are the key advantages and disadvantages of a Deferred Prosecution Agreement ("DPA")?

31 Q10. What impact, if any, will Brexit have on UK and European fraud & white collar crime efforts?

Meet The Experts

Hidetaka Miyake - Anderson Mori & Tomotsune
T: +81-3-6775-1121
E: hidetaka.miyake@amt-law.com

Hidetaka Miyake is one of the leading lawyers in the fields of government investigations and crisis management in Japan. By leveraging his background as a former public prosecutor, a former senior investigator at the Securities and Exchange Surveillance Commission and a former forensic senior manager of a Big Four accounting firm, he focuses on handling internal or independent investigations for listed companies to address complex accounting frauds. He also handles crisis management for financial institutions and criminal defense for non-Japanese clients. Since joining Anderson Mori & Tomotsune in 2017, he has been involved in accounting fraud investigations for more than 10 Japanese listed companies.

Aisling O'Sullivan - Brown Rudnick LLP
T: +44 (0) 207 851 6080
E: aosullivan@brownrudnick.com

Aisling O'Sullivan is an associate in the White Collar Defense & Government Investigations practice group, based in London. Her practice focuses on compliance, corporate crime, investigations and civil litigation, including asset tracing and recovery. Aisling is part of Brown Rudnick's Supervising Solicitors team having relevant experience in the execution of search/delivery up orders.

Aisling provides advice and representation to corporates and individuals facing criminal and regulatory enforcement action. She has acted on investigations led by UK and international agencies into allegations of fraud, bribery and corruption, false accounting and money laundering. Aisling also has experience in requests for mutual legal assistance and extradition, relating to the investigation and prosecution of criminal offences abroad.

In the context of compliance, Aisling advises clients on financial crime and risk management. She has experience in conducting risk assessments and implementing compliance manuals, programs and policies to comply with a range of legal and regulatory obligations.

Aisling has particular experience in complex cross-border civil litigation, providing strategic advice to clients to trace and recover assets overseas.

Prior to joining Brown Rudnick, Aisling was an associate at a top tier US law firm, having previously trained and practiced at an international law firm. Before entering private practice, Aisling worked in the equity derivatives division of a US investment bank, focusing on equity swaps for hedge funds, asset managers and corporates.

Kevin Sweeney - Chamberlain Hrdlicka
T: +1 610.772.2327
E: ksweeney@chamberlainlaw.com

Kevin Sweeney is an experienced tax attorney and former federal prosecutor who specializes in defending clients in civil and criminal tax controversy and litigation matters. He focuses on high-stakes IRS audits, civil tax litigation, white-collar criminal defense and investigations, and whistleblower matters for high and ultra-high net worth individuals, corporate executives, business owners, and public and private companies worldwide. Prior to transitioning to private practice, Kevin was part of a select team of U.S. Department of Justice attorneys who specialized in tax investigations and prosecutions of foreign companies and financial institutions.

Meet The Experts

Neil Keenan - Forensic Risk Alliance
T: +44 (0)20 7831 9110
E: nkeenan@forensicrisk.com

Neil Keenan is a Partner at FRA based in the firm's Washington DC office. He has considerable experience providing accounting and advisory services to clients across a variety of industries, and geographies.

Neil specializes in the delivery of forensic accounting services including accounting fraud, audit/accounting malpractice litigation, anti-corruption investigations and compliance, and asset misappropriation and embezzlement.

Over the past 23 years, Neil has built strong relationships with his clients through his discipline, professionalism, and loyalty. As a Forensic Services professional he brings an intense focus and vision for developing and executing practical strategies to resolve complex client issues.

Beyond investigations, Neil brings broad experience that includes claims processing, M&A financial and compliance due diligence, corporate finance, corporate valuations, business recovery and restructurings, and external and internal audit services.

Ian Herbert - Miller & Chevalier
T: +1-202-288-2044
E: iherbert@milchev.com

Ian Herbert focuses his practice on white-collar criminal investigations and litigation, representing both companies and executives through interactions with government prosecutors and regulators. He has significant experience representing financial services companies and employees, including offshore trust companies, in US-based and cross-border investigations.

Arantxa Geijo Jimenez - Geijo & Associates SLP
T: +34673845710
E: arantxa@geijoandassociates.com

Arantxa Geijo Jiménez, founder and managing partner of Geijo&Associates SLP, is a Spanish attorney who is an expert in international law, particularly in international criminal law and human rights law. In addition to her practice, she is also currently Of Counsel at Freeh Sporkin & Sullivan, LPP, where she handles international criminal law cases for that firm.

She has previously served as counsel for the INTERPOL General Secretariat Office of Legal Affairs at their headquarters in Lyon, France, where she focused on complex international criminal arrest warrant requests (Red Notices) and represented INTERPOL in litigation, including challenges by individuals to the issuance of Red Notices against them.

Arantxa has served as an attorney at prestigious law firms in Madrid and London. She is also an associate professor of Law at Valencia International University.

James Garrett - ApiJect Systems, Corp
T: +1-619-750-3121
E: jgarrett@apiject.com

James Garrett is the newly appointed General Counsel and Chief Compliance Officer at ApiJect Systems, Corp., a medical technology company that is working to develop surge capacity for supplying vaccines and medicines in individual doses for injection. Prior to joining ApiJect, Mr. Garrett held various executive positions at NuVasive, Inc., including senior vice president, government and regulations strategy, where he was responsible for designing and executing non-market strategies to assess opportunities and threats that may impact business results. His prior role at NuVasive was leader of business and quality systems, responsible for global risk and integrity, regulatory affairs, quality affairs, information technology, and environmental health and safety. He also served as the organization's chief risk and compliance officer, and associate general counsel.

Dennis Miralis - Nyman Gibson Miralis
T: +61 2 9264 8884
E: dm@ngm.com.au

Dennis Miralis is a leading Australian defence lawyer who specialises in international white collar crime law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions.

His areas of expertise include fraud, white collar crime, bribery and corruption, global tax investigations, proceeds of crime, anti-money laundering, worldwide freezing orders, extradition and mutual legal assistance law.

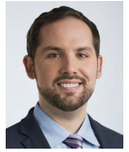
Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.

Q1. Have there been any recent regulatory changes or interesting developments?

Dennis Miralis

Miralis: Jurisdictions across the Asia-Pacific region are moving towards stronger and more complex legal and regulatory frameworks to combat fraud and white collar crime, including corruption and bribery, which often has an international dimension. This poses a challenge for companies who operate international businesses as they must ensure that they are fully aware of the local laws that govern white collar offences, the laws of their home jurisdiction which may have extra-territorial effect on their businesses, as well the laws of third jurisdictions which may also similarly have extra territorial effect.

One example of this is how Asia-Pacific jurisdictions are implementing further measures to hold legal persons liable for criminal conduct by natural persons and to incentivise companies to develop sufficient anti-corruption policy. Corporations often stand to financially benefit from bribery and corruption, and so prosecution against natural persons is insufficient. For example, the Australian Government has proposed reform to Australian foreign bribery laws including introducing an offence for corporations that fail to prevent foreign bribery.[1] In Singapore, companies can be liable for crimes committed by an individual who is 'the embodiment of the company' (primary liability) or who acts 'within the scope of a function of management properly delegated' (vicarious liability).'[2] In the PRC, the Amended Anti-Unfair Competition Law (AUCL) 2018 Article 7 states that 'bribery committed by a staff member of a business operator shall be deemed the conduct of the business operator, unless the business operator has evidence to prove that such acts of the staff member are unrelated to seeking business opportunities or competitive advantage for the business operator'. Similar legislation has been implemented and or is being considered in many other jurisdictions.



Ian Herbert

Herbert: On 1 January 2021, Congress made some of the biggest changes to U.S. anti-money laundering ("AML") laws in recent memory with the passage of the National Defense Authorization Act, an omnibus spending bill that included Corporate Transparency Act and the Anti-Money Laundering Act of 2020.

The new legislation makes a number of important changes to the AML laws, and we have been fielding a lot of questions about its impact. The primary change is that the law will require many companies created under the laws of the United States and registered to do business here to report to FinCEN the identity and personal identifying information of each beneficial owner. The focus of the law is on private companies, and U.S. issuers are exempted, as are other regulated entities such as banks and credit unions, but it is still expected to have a significant impact and will go a long way towards bringing the U.S. in line with international AML standards on beneficial ownership. Under the law, a beneficial owner is anyone who owns more than 25% of, or exercises substantial control over, the entity (though there are some exceptions that will be important as the law gets implemented through regulations).

The new legislation makes a number of other important changes to the AML laws, and it would be difficult to discuss all the changes here, but I wanted to quickly highlight a couple other key changes. First, the law gives the Treasury and DOJ authority to issue subpoenas to any foreign bank with U.S. correspondent accounts. Those subpoenas can require the production of information related to any account at the foreign bank, whereas previously only information about the correspondence U.S. accounts could be subpoenaed. Second, the rewards for and protection of whistleblowers have also been enhanced. Previously, the reward for a whistleblower who provided non-public information to FinCEN was capped at 25% or $150,000, whichever was lower. The new law increases the cap to 30% of all monetary sanctions collected, without any cap, and mandates that the Secretary of Treasury "shall" pay an award for actions that result in monetary sanctions over $1 million. The new legislation also adds anti-retaliation protections for whistleblowers.

1. Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, Crimes Legislation Amendment (Combating Corporate Crime) Bill 2019 (2020), 13.
2. See Tom Reck Security Services Pte Ltd v Public Prosecutor (2001) 2 SGHC 72.

Arantxa Geijo Jimenez

Jiménez: The European Union (EU) has strengthened its stance against fraud & white collar crime. Notable developments include the establishment of the EU Public Prosecutor's Office ("EPPO"), an independent body of the EU with the authority to investigate, prosecute and bring to justice crimes against the EU budget. The EPPO was established by Council Regulation (EU) 2017/1939 of 12 October 2017, implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office.

The EPPO is a supranational prosecutorial body, the first of its kind. The EPPO will investigate and prosecute crimes affecting the EU's financial interests as set out in Directive 2017/1371 of 5 July 2017 on the fight against fraud to the Union's financial interests by mean of criminal law (the "PIF Directive"). These crimes against the EU budget include corruption and fraud, including VAT fraud. There are currently 22 Member States participating in the EPPO, and non-participating Member States can join at any point.

The establishment of the EPPO is an unprecedented step in the fight against cross-border financial crime. Its objective is to enhance cooperation among participating states to better combat fraud. However, it may also have an effect on non-participating Member States as well as states outside of the EU. Indeed, in accordance with its establishing regulation, the EPPO may seek cooperation and agree to working arrangements with non-participating Member States and other countries where entities or individuals are involved, or are suspected to be involved, in the commission of a crime against the EU budget.

It is also worth mentioning Directive 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law (the "Whistleblower Directive"), which must be transposed into national law by 17 December 2021. The aim of the Whistleblower Directive is to afford protection to persons who report breaches of EU law. The Directive affects public and private organisations with 50 or more employees and imposes a number of obligations on those entities, including the adoption of safe reporting channels and measures to protect whistleblowers from retaliation. This could be significant for Member States that lack a legal framework for whistleblower protection, such as Spain, which could capitaliae on the existing framework of the Directive to include breaches of national legislation, in addition to EU law.

Neil Keenan

Keenan: One recent development could have significant impact on the U.S. Securities and Exchange Commission's ("SEC") ability to seek disgorgement of any unjust enrichment resulting from a violation of a securities law. On 11 December 2020, Congress passed the National Defense Authorization Act for Fiscal Year 2021 ("NDAA"). The NDAA includes language amending the Securities Exchange Act of 1934 (the "Exchange Act") granting the SEC with express statutory authority to seek disgorgement in civil enforcement actions, and doubling the statute of limitations for disgorgement from five to 10 years. As we know, the SEC frequently seeks to disgorge illicit profits in Foreign Corrupt Practices Act resolutions, and this new legislation provides the SEC with the clarity and explicit approval to pursue ill-gotten gains in federal court.

This represents a direct congressional response to limitations imposed by the Supreme Court in both *Liu v. SEC* (140 S. Ct. 1936 (2020)) and *Kokesh v. SEC (*137 S. Ct. 1635 (2017)). In *Kokesh v. SEC*, the Supreme Court ruled that the disgorgement of ill-gotten gains constituted a penalty and, therefore, were subject to the five-year statute of limitations period. This restricted the SEC's ability to recover funds for victims if the fraudulent scheme commenced more than five years earlier. While the Kokesh ruling did not opine on whether the SEC had the explicit authority to seek disgorgement in the first place, the Supreme Court ruling in *Liu v. SEC* determined that the SEC did indeed have the power to seek disgorgement in federal court. However, the Court limited the recoverable amount to the net profit obtained from the unlawful conduct.

Q1. Have there been any recent regulatory changes or interesting developments?


Dennis Miralis

The full scope and impact of these amendments remain to be seen, and will likely require case law development that may not be long in coming. If enacted, the amendments to the Securities Exchange Act included in the NDAA will be applicable to not just future cases but also to those currently pending. For those cases where illicit profits have been 'earned' by wrongdoers over many years, the return of 10 years' worth of ill-gotten gains could well result in a significant increase to the size of payments being made by the targets of SEC disgorgement actions. It will, however, be interesting to see how courts potentially restrict disgorgement amounts to the equitable limitations identified in Liu.


Kevin Sweeney

Sweeney: On 1 January 2021, Congress passed the Anti-Money Laundering Act of 2020 ("AMLA" or "Act"). The AMLA provides significant reforms to the Bank Secrecy Act ("BSA"), which is the United States' seminal anti-money laundering law. The AMLA has the potential to increase enforcement of BSA/AML laws against companies and individuals through data gathering, information-sharing, and cross-border coordination in numerous ways including the following:

- Expanding AML/BSA whistleblower awards from a maximum of $150,000 to up to 30% of monetary sanctions over $1 million collected by the U.S. Department of Justice ("DOJ") or U.S. Treasury Department;
- Creating new penalties for those who conceal material information from financial institutions concerning the source of and/or control over certain funds and assets and enhancing penalties for existing AML and BSA violations;
- Expanding DOJ and the Treasury's existing authority to subpoena foreign banks for records related only to correspondent accounts in the U.S. to any account at that foreign bank including records maintained outside the U.S. provided that the records are the subject of an investigation relating to U.S. criminal law violations, BSA violations, civil forfeiture, or Section 5318A;
- Providing for increased staffing of government agencies responsible for BSA/AML oversight and enforcement;
- Creating a pilot program to facilitate the sharing of Suspicious Activity Report ("SAR") information with foreign counterparts;
- Relieving financial institutions of liability if they cooperate with law enforcement requests to keep accounts open for law enforcement monitoring purposes;
- Requiring DOJ to report to Congress on AML Deferred Prosecution Agreements and Non-Prosecution Agreements on an annual basis;
- Creating a Treasury Attaché program in U.S. embassies to establish relationships with foreign counterparts and liaison positions to perform BSA officer outreach;
- Expanding the definition of "money transmitting business" under the BSA to include businesses engaged in the exchange or transmission of "value that substitutes for currency" such as virtual currency and the definition of "financial institutions" under the BSA to include antiquities dealers, advisors, and consultants;
- Requiring smaller companies to disclose beneficial ownership to the Financial Crimes Enforcement Network ("FinCEN"), which is shareable with financial institutions for customer due diligence purposes upon consent of the reporting company.


Hidetaka Miyake

Miyake: In recent years, disclosure regulations that apply to listed companies in Japan have been gradually tightened. In particular, the Financial Services Agency ("FSA") is making vigorous efforts to enhance the disclosure of non-financial information in the annual securities reports prepared and submitted by listed companies under the Financial Instruments and Exchange Act ("FIEA"), such as information regarding executive compensation, management policies and strategies, and business risks.

In line with such efforts by the FSA, there have been a number of enforcement cases in which the Securities and Exchange Surveillance Commission ("SESC") had found material false statements of non-financial information in securities reports that violated the disclosure regulations under the FIEA. For example, in December 2019, the SESC closed its investigation of a listed company's disclosure documents and recommended that the FSA take an administrative action ordering the company to pay an administrative monetary penalty of 24 million yen for making material false statements in its financial statements as well as in the "Status of Corporate Governance" section of its securities report.

In this case, the securities report had stated that the board meetings were held monthly and that certain important items were discussed in the meetings, but the SESC's investigation found that the board meetings were actually only held three times a year, and most of the important items were not discussed in the meetings. The SESC's previous enforcement actions had mainly focused on the detection of material false statements of financial information. Going forward, however, the number of enforcement cases in respect of material false statements of non-financial information is expected to increase.

Q2. Are there any compliance issues or potential pitfalls that firms need to be cautious about?


James Garrett

Garrett: The most common pitfall I believe that most companies fall into is having the belief that the risk of fraud is mitigated because they have policies and procedures in place to address that risk. Said another way, policies can create complacency and their needs to be a concerted and constant effort on behalf of management to reinforce and explain the rationale behind policies and procedures that address fraud and abuse.

Simply having a policy or even a detailed compliance programme is not enough to mitigate risk, much less drive value from compliance. Employees need to understand that integrity matters and that anything less is unacceptable. Policies, procedures and certain practices need to be refreshed on a regular basis and employees need to "practice" them in the same way the most successful sports teams practice, practice and practice again before game time.


Ian Herbert

Herbert: Several U.S. financial agencies have issued informal guidance over the past few months related to AML and Bank Secrecy Act enforcement that will affect the way entities, particularly financial institutions, deal with AML compliance. In this context, we have noticed that agencies want entities to take a risk-based approach to evaluating the compliance programmes for banks and other financial institutions, rather than apply a one-size-fits-all solution.

In April 2020, the Federal Financial Institutions Examination Counsel revised its examination manual to reinforce the risk-based approach to compliance programme examinations. Then, in August, a number of federal agencies, including FinCEN and the OCC, issued a joint statement on due diligence requirements for customers that the financial institution may deem politically exposed persons. The statement answered specific questions about who should be treated as politically exposed persons (for example, it said that the agencies do not interpret the term to include U.S. public officials), and then emphasised the need to apply a risk-based approach to customer due diligence when evaluating customers. The statement said that there is no requirement in regulations and no regulator expectation for banks to have additional due diligence steps for PEPs but that PEP relationships present varying levels of money laundering risk depending on other factors. The agencies were clear that banks must adopt appropriate risk-based procedures for conducting customer due diligence based on the totality of those factors.

Q2. Are there any compliance issues or potential pitfalls that firms need to be cautious about?


Ian Herbert

Also in August, the FDIC, OCC and other agencies issued a joint statement regarding when cease and desist orders are appropriate against financial institutions. One of the primary justifications for a cease and desist order is failure to establish and maintain a reasonably designed AML compliance programme, and the guidance talked repeatedly about the need to use a risk-based approach in creating and maintaining those compliance programmes. Tailoring compliance programmes to an entity's specific risks is not a new concept for compliance officials and their advisors; what is new, or at least renewed, is the explicit focus by the key agencies.


Neil Keenan

Keenan: I think that the past year has been interesting in terms of the nature of cases surfacing, most notably in Europe. Several European listed companies have disclosed false accounting and/or reporting of cash and cash equivalents, and/or financial debt levels. Most notably, Wildcard, NMC Health and Finablr.

Due to the availability of third party evidence to corroborate bank, cash and debt levels—via bank statements, contracts and bank confirmations—many may believe that such areas are very well controlled, and represent a low level of risk to an organisation. Indeed, many auditing firms assign responsibility for auditing bank and cash to the most junior members of the team. The scale and duration of those schemes noted above, each in excess of $1 billion and running for several years, should make corporations and their boards re-evaluate how they view risks surrounding the treasury function, not just from a liquidity perspective but also the existence of and operation of basic internal controls and reporting. This may be heightened during the on-going pandemic as companies face liquidity issues, may seek alternative sources of funding and feel the need to portray a healthier balance sheet and cash position than perhaps is true. Boards should also assess the existence of alternative financing sources, including supply chain financing arrangements (often referred to as reverse factoring), that may not be fully disclosed, but which may increase not only reporting disclosure risks but future liquidity issues.

Within the U.S., an interesting development that we are tracking is the SEC's earnings per share, or EPS initiative. Launched in 2018, the Wall Street Journal reported that the SEC had initiated probes into several companies that had potentially rounded up their reported Earnings per Share ("EPS"). In October 2020, at least two of these companies have been charged with "improper reporting of quarterly earnings per share" in order to meet or exceed analysts' consensus estimates. When analysing such cases, both companies experienced periods of consistently meeting or exceeding EPS targets, followed by a subsequent significant drop in earnings that failed to meet market expectations by a considerable margin. While the SEC has consistently looked for and brought earnings management cases, I anticipate that this will be a continued focus, with the SEC asking whether companies with considerable decline in performance inappropriately used the pandemic to mask previously overstated balance sheets and financial performance. Comparing your company's performance relative to peer companies may be beneficial as I believe regulators including the SEC, with their enhanced analytical tools, may be doing the same.


Kevin Sweeney

Sweeney: Firms need to be careful to avoid implementing a one-size-fits-all compliance programme, to continuously review and tailor the programme to their unique needs, and to ensure adequate resources and autonomy for compliance. On 1 June 2020, the DOJ updated its guidance document titled "*Evaluation of Corporate Compliance Programs*". This update offered additional insights into the factors that DOJ will prioritise in its evaluations of corporate compliance programmes. It emphasised continuous review of and data-driven updates to a company's compliance programme, which should be carefully tailored to the particular circumstances of the company at issue and adequately resourced and empowered.

The DOJ's focus on continual data-driven improvement suggests a desire to encourage rather than punish companies to remediate gaps and areas of vulnerability in the compliance function. Moreover, its emphasis on processes for tracking and utilising data analytics reflects an expectation that companies will use available data to attempt to spot such gaps and vulnerabilities. Finally, the guidance's focus on whether the compliance programme is "adequately resourced and empowered to function" suggests that, in addition to reviewing the programme itself, the DOJ intends to scrutinise the company's efforts to effectively implement, fund, and grant autonomy to the company's compliance function.


Aisling O'Sullivan

O'Sullivan: Many of the compliance issues that arose throughout 2020 will remain in place. For example, remote working and the associated compliance risks around fraud, cyber-security, data protection, and the lack of consolidated oversight. Brexit, however, presents new compliance issues as companies across a range of industry sectors grapple with the recently implemented Trade and Cooperation Agreement and the resulting legislative and regulatory changes.

More generally, the near universal need for businesses to reduce costs in the wake of the COVID-19 pandemic will undoubtedly have had a negative impact on compliance budgets. Such cuts inevitably hinder the ability of companies to prevent and detect misconduct and compliance breaches. Companies therefore need to ensure that compliance is not neglected in budgets and/or business continuity plans.

Compliance functions also need to continue to demonstrate agility by quickly adapting to the rapidly evolving work landscape. For example, the UK's extensive work-from-home arrangements have forced compliance outside of the office and as such, it has become a necessity (as opposed to an often-overlooked luxury) as staff access systems remotely and risks to data security increases. In addition, remote working has presented general health and safety issues and mental health (including risks and bullying/ harassment risks) that firms need to continue to be mindful of.

Finally, the arrival of COVID vaccines presents another compliance headache as the burden of maintaining sensitive data related to employee health takes on a new form. Initially, companies had requested that employees inform them if they were ill with COVID or exposed to an infected person which could likely put other employees at risk. In some sectors, particularly those in healthcare, the question of whether employees can attend their place of work without proof of vaccination is likely to become an issue. Companies will need to ensure that employee data pertaining to COVID -19 is managed in accordance with local data protection laws.


Hidetaka Miyake

Miyake: Officers and employees of Japanese listed companies should pay particular attention to the risk of insider trading. Although insider trading regulations were introduced in Japan in 1988, only those who carried out transactions in possession of non-public material information were subject to the regulations. This means that the so-called "tipper liability" was not stipulated under the regulations. However, the 2013 amendment to the FIEA, which came into effect in April 2014, introduced new insider trading regulations on information disclosure and trade recommendations.

The new regulations introduced a ban on disclosing non-public material information to any person, or making trade recommendations to any person, for the purpose of encouraging such person to make a profit or avoid a loss. In this regard, an important point to keep in mind is that corporate insiders in possession of non-public material information may be in breach of the new regulations simply by recommending a trade to a third party without disclosing the non-public material information.

Q2. Are there any compliance issues or potential pitfalls that firms need to be cautious about?


Hidetaka Miyake

Since the introduction of the new regulations, the SESC has been actively detecting illegal trade recommendations and raising public awareness of the risks of insider trading, but some executives and employees of listed companies still do not fully understand the importance of the new regulations and the accompanying compliance risks. For example, the Tokyo Public Prosecutors Office and the SESC recently jointly investigated a former CEO of a famous listed company regarding alleged illegal trade recommendations, and the former CEO was indicted in December 2020.

According to the news reports, the former CEO was not aware of the regulations on illegal trade recommendations. In this respect, listed companies should be aware of the risks of making illegal trade recommendations and revisit their internal policies and procedures to check if they adequately address such risks.

Q3. Have there been any noteworthy case studies or examples of new case law precedent?


Dennis Miralis

Miralis: Criminal investigations are increasing across international borders, requiring countries to cooperate and coordinate their efforts in order to combat transnational crime as evidenced by global efforts to investigate and combat cartel conduct.

On 2 September 2020, five countries including Australia entered a new memorandum of understanding called the Multilateral Mutual Assistance and Cooperation Framework for Competition Authorities ("MMAC"). The agencies participating in the MMAC are the U.S. Department of Justice, U.S. Federal Trade Commission, UK Competition and Markets Authority, New Zealand Commerce Commission, Competition Bureau Canada, and Australian Competition and Consumer Commission ("ACCC").

The MMAC was created in order to improve cooperation between parties through provision of mutual assistance, sharing of confidential information, execution of searches and seizures, and cross-border evidence gathering.

While a memorandum of understanding is not legally enforceable, it acts as a sign of commitment between parties and a show of intent to cooperate in borderless white collar crime.


Ian Herbert

Herbert: One interesting case from the end of last year was the Goldman Sachs FCPA resolution. With a total of $2.9 billion paid to resolve cases brought by multiple regulators in multiple countries, it was the largest ever FCPA settlement. But that's not really why it was interesting in my mind. Two aspects that stuck out to me were the effect that a company's cooperation and its compliance programme enhancements can have on a resolution like this.

Regarding cooperation, we have a great case study because the result in Goldman can be compared to that in Airbus, the second biggest FCPA settlement ever, from earlier in 2020. Both Goldman and Airbus faced potential criminal fines under the sentencing guidelines between $2.789 billion and $5.579 billion. However, Airbus received a 25% discount for its cooperation and remediation, the maximum permitted for companies that do not self-disclose under the DOJ's FCPA Corporate Enforcement Policy. Goldman, on the other hand, received only a 10% reduction despite providing "all relevant facts known to it." According to the DPA, Goldman did not receive full cooperation and remediation credit because of "significant" delays in providing cooperation. Particularly in light of the size of the penalties at issue, the difference in cooperation discounts tangibly demonstrates the impact of the DOJ's assessment of "full cooperation." The Airbus criminal fine was the bottom of the guideline range reduced by 25% for its cooperation, for a total fine of $2.091 billion. Goldman, with the same guideline range, had to pay $225 million more ($2.315 billion), plus disgorgement.

A second aspect that was interesting was that Goldman managed to avoid an independent compliance monitor despite significant shortcomings in its compliance programme at the time of the offences. Goldman had a compliance programme that subjected each bond transaction to layers of review under the Company's internal accounting controls, including reviews by internal committees. But still the controls were circumvented or inaptly applied, which allowed someone who the control functions had identified as posing a significant risk to participate in the transactions leading to significant bribe payments. Despite those compliance failings, Goldman avoided a monitor, which was a significant win for the company and clearly tied to significant compliance programme enhancements it instituted during the investigation.

At Miller & Chevalier, our preferred approach is to include our compliance experts in our investigations so that, if needed, remediation can begin while the investigation is still on-going. The Goldman resolution is a good demonstration of why that is the case.


Neil Keenan

Keenan: While my response does not discuss new case law precedent, it is perhaps the lack of case law, highlighted by two SEC Commissioners, Commissioners Peirce and Roisman, in a 13 November 2020 Statement that might be of interest. In a somewhat unusual development, the two Commissioners released a statement to explain why they voted against the Commission's settled action in the matter of Andeavor.[1]

Andeavor was adjudged to have violated Exchange Act Section 13(b)(2)(B), which requires reporting companies to devise and maintain a system of "internal accounting controls," when it repurchased its stock from shareholders after its legal department concluded that it did not possess material non-public information about a merger. The Commissioners dissented on the basis that the SEC may be applying an "unduly broad view of Section 13(b)(2)(B)" in charging public companies. The Statement points to the lack of case law on which to draw, citing "[n]o court... has adopted the expansive view of Section 13(b)(2)(B)" that some SEC actions seem to require. This may, perhaps, be on account of a company's willingness to accept what is viewed as the lessor "controls violation" charge as compared to a more serious violation, such as corruption, or in the Andeavor matter, insider trading.

The Commissioner's dissent focuses on the apparent interpretation of the Section as a company's need to meet general internal controls, as opposed to the actual language in the provision that references "internal accounting controls." The "internal accounting controls" provision was enacted in the Foreign Corrupt Practices Act ("FCPA"), and in drafting such legislation it appears that the language considered definitions contain in Statements of Auditing Standards published by the AICPA. Such Standards differentiate between "accounting controls" and "administrative controls." The Standard states that "accounting controls... generally bear directly and importantly on the reliability of financial records and require evaluation by the auditor," while "[a]dministrative controls... ordinarily relate only indirectly to the financial records and thus would not require evaluation."

Those who observe SEC settlements will note that many cases are settled by companies accepting an "internal controls" violation. It will be interesting to see if companies, perhaps empowered by the recent statement by the Commissioners, will elect to challenge the SEC on their definition of "internal accounting controls" or will choose not to do so, accept such charges in order to resolve matters, and move forward.

1. *See Exchange Act Release No. 90208 (15 Oct 2020), https://www.sec.gov/litigation/admin/2020/34-90208.pdf*

Q3. Have there been any noteworthy case studies or examples of new case law precedent?


Kevin Sweeney

Sweeney: One noteworthy case for corporations facing tax evasion probes is *United States v. Hapoalim (Switzerland) Ltd.*, which was resolved by a Deferred Prosecution Agreement ("DPA") in April 2020. Pursuant to this Agreement, Bank Hapoalim agreed to pay $874 million in back taxes, forfeiture, and penalties, which was the second largest corporate tax evasion resolution since 2008.

Notably, the DOJ press release cited Bank Hapoalim's deficient early cooperation, which began in 2011, as a reason for the severity of its penalty. In particular, it noted that the bank had initially conducted an inadequate internal investigation, failed to disclose relevant facts on time and, at times, provided incomplete and inaccurate information to investigators. More specifically, according to public documents, it wasn't until 2017 that Bank Hapoalim hired an external accounting firm to assist in its internal review, which frustrated DOJ's efforts to punish individuals allegedly linked to the scheme.

This case demonstrates that any company that decides to cooperate with DOJ should promptly hire an appropriate investigative team, conduct a thorough investigation, and promptly respond to DOJ requests. Anything less could subject it to increased and unnecessary punitive exposure.


Hidetaka Miyake

Miyake: Recently, the scandal involving Mr Carlos Ghosn, a former chairman of Nissan Motor Co., Ltd. (Nissan), has attracted attention around the world. On 19 November 2019, Mr Ghosn was suddenly arrested on suspicion of violating the FIEA by understating his remuneration in Nissan's annual securities reports for five years. Mr Ghosn was later indicted on 10 December 2019 for FIEA violations, but was rearrested on the same day for understating his remuneration in Nissan's annual securities reports for another three years. Mr Ghosn's case was then investigated by the Special Investigation Division of the Tokyo District Public Prosecutors Office, which specialises in serious white-collar crimes.

Under Japan's criminal justice system, an accused may be detained for a period of 10 days during an investigation, but at the request of a public prosecutor, judges may extend the detention period for up to 10 more days. This has led to many cases where the detention of suspects is often prolonged, and Japan's criminal justice system has therefore sometimes been criticised as being a system of "hostage justice". In particular, in cases where investigations are carried out by the Special Investigation Division, a prosecutor's request for an extension of detention has typically been approved by the judge almost without exception in practice.

However, in Mr Ghosn's case, the Tokyo District Court rejected the prosecutor's request for an extension of his detention on 20 December 2019, and the prosecutor's appeal was also dismissed. Although Mr Ghosn was eventually rearrested on 21 December 2019 on the ground of aggravated breach of trust and finally released on bail on 6 March 2020, 108 days after his arrest, the court's decision to dismiss the prosecutor's request for an extension of Mr Ghosn's detention can be seen as a sign of a change in the practice of long-term detention in Japan.

"Under Japan's criminal justice system, an accused may be detained for a period of 10 days during an investigation, but at the request of a public prosecutor, judges may extend the detention period for up to 10 more days."
- Hidetaka Miyake -

Q4. How has COVID-19 impacted the fraud & white collar crime landscape?


Dennis Miralis

Miralis: COVID-19 has led to a surge in fraud and white collar crime and in particular has increased money laundering risks. The Financial Action Task Force (FATF) sets international standards to combat global money laundering and terrorist financing, and has highlighted some of the issues emerging.[1]

FATF highlights the current landscape of increased fraud and white collar crime due to COVID-19 as affected by the increased reliance on online systems for remote work, purchase of products and social interaction, the increased demand for medical supplies, and the diversion of government resources towards COVID-19 management.[2]

Criminals may impersonate government officials (e.g. hospital officials, to retrieve personal banking information), as criminals may attempt to profit off increased government relief to citizens. There is also an increase of scams over essential goods and medical supplies due to the increased need. This can include non-delivery of items, delivery of counterfeit or defective goods, or marketing of misleading and false COVID-19 treatments and cures.[3]

FATF also notes an increase in fundraising scams requesting donations for COVID-19-related fundraising, and investment scams including for false COVID-19 treatments. Criminals also pose as official organisations such as the World Health Organization to lure users through email and SMS to reveal or have their data leaked, or use malicious websites that pose as sharing pandemic information to lock user's electronic devices until ransom payment is made.[4]


James Garrett

Garrett: The impact of COVID-19 has impacted the fraud and white collar crime landscape in the same way that it has impacted all of our lives. Governmental and regulatory oversight, monitoring and auditing targeted to preventing or uncovering fraud has, in many cases, slowed down as resources are diverted (or at least distracted) with efforts to fight the pandemic. The same is true for many companies around the globe who are struggling to manage their business and – in some cases – keep their doors open in the face of an unprecedented economic downturn.

Compounding the problem, unemployment is up and (at the very least) those that are still employed may be nervous about their financial future. All of these issues exacerbate the potential for fraud and white collar crime and create an environment ripe with potential for abuse, as well as the likelihood that any fraud that is perpetuated will not be quickly uncovered or mitigated.


Ian Herbert

Herbert: I suspect that COVID-19 will have a significant impact on fraud and white collar prosecutions, and we have already seen the beginning of that in the US. In March 2020, Congress passed the CARES Act, a $2.2 trillion stimulus bill. The stimulus included, among other things, nearly $700 billion in forgivable loans to small businesses under the Paycheck Protection Program and $500 billion in additional aid for corporations. Almost as soon as those programmes were implemented, we began seeing enforcement actions against individuals and entities attempting to defraud beneficiaries.

In May 2020, the DOJ charged a Texas man with wire fraud, bank fraud, and related charges for seeking $5 million from the PPP programme by falsely claiming to have 400 employees and an average monthly payroll of $2 million. By September 2020, the government had charged more than 50 individuals of trying to fraudulently receive $175 million from the PPP programme. In addition to the stimulus related prosecutions, federal prosecutors have sought to crack down on securities and health care fraud scheme stemming from the coronavirus pandemic.

1. http://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf
2. Ibid 5–6
3. Ibid 6–7
4. Ibid

Q4. How has COVID-19 impacted the fraud & white collar crime landscape?

Ian Herbert

We have also seen that, after some initial delays at the start of the pandemic, the enforcement agencies have found their footing and have found ways to investigate and bring fraud and white collar cases. Virtual proffers and interviews are now done on a routine basis and cases continue to be brought, albeit on a somewhat slower pace. As an overall matter, white collar criminal cases have fallen off in demonstrable ways during the Trump administration, but COVID-19 has not been the primary driver of that.

Arantxa Geijo Jimenez

Jiménez: Sudden changes in the economic and social environment invariably create uncertainty and regulatory gaps, which those seeking to commit fraud will seek to exploit. The COVID-19 global crisis is no different.

The COVID-19 crisis has thus changed the fraud and white collar crime landscape, at least in the short-term, in two manners. Firstly, it has paved the way for new financial crime risks and typologies adapted to the current situation. Secondly, it has had an impact on law enforcement activities.

For instance, COVID-19 has triggered a surge in counterfeit medical supplies and medicines, cybercrime (such as malware and ransomware), online and telephone fraud seeking victims to provide payments details or open malware attachments, and espionage.

New financial crime risks can largely be associated to remote working conditions. For instance, from an anti-money laundering perspective, teleworking increases the risk of fraud. Indeed, the inability to hold in-person meetings widens the scope for fraud through the submission of falsified documents and pictures online. This issue is particularly concerning for companies whose internal processes were not digitalised in the wake of lockdown measures. In addition, it may be harder to supervise personnel who are working remotely and ensure adherence to compliance and vetting procedures. Given the current economic environment, it is also worth noting that there is a real risk that a continuous influx of profit is prioritised over a rigorous approach to anti-money laundering checks and procedures.

Moreover, the increase of government schemes that provide financial support for businesses combined with the weakening economic climate has also created the potential for abuse and fraud in relation thereof.

Law enforcement activity has equally been affected by decreased mobility and remote working. Financial crime investigations and prosecutions have slowed down. To begin with, judicial activity was significantly reduced during the first wave of national lockdowns. For instance, in Spain, administrative and judicial proceedings were suspended from 14 March until June 2020, subject to limited exceptions.

Equally, social distancing requirements have encumbered the evidence gathering process. For example, in person consultation between criminal defendants and their attorneys have been adversely affected, including restricting measures put in place to prevent infections during in person witness interviews. Witness interviews are largely conducted through digital channels and confidentiality concerns over digital communications also arise.

Kevin Sweeney

Sweeney: COVID-19 has placed an incredible amount of strain on the U.S. judicial system. Federal courthouses across the nation have streamlined their normal operations significantly. Courts have been prioritising criminal cases with detained defendants and those that implicate speedy trial issues, which are not typical in white collar cases. Moreover, jury trials have more or less been halted, which has resulted in a significant backlog of cases. This backlog may take several years to clear. In light of this backlog, some prosecutors may be discouraged from filing new cases involving complex factual issues.

The pandemic has also slowed pending investigations. Concerns for the health of federal law enforcement agents and other government employees has resulted in fewer search warrants and "knock and talks." Moreover, social distancing impeded work with cooperating witnesses, because prosecutors and investigators prefer multiple in-person meetings to create trust and evaluate witnesses. Additionally, the difficulties in convening grand juries has complicated the process of compelling testimony necessary for prosecutors to build their cases. While law enforcement can still utilise subpoenas for documents to build white collar cases, many recipients have good reason for requesting an enlargement of time to respond, which can further delay such investigations.

With respect to corporate investigations, work-from-home restrictions, employee furloughs, and diminishing resources have strained the abilities of companies to comply with subpoenas. Moreover, these considerations have made it more difficult to conduct internal investigations, which has delayed self-reporting. Additionally, the economic uncertainties brought about by COVID-19 have impacted the government's ability to reach resolutions with companies, which must assess their own financial condition before engaging in meaningful discussions about fines or settlements. This slowdown in white collar enforcement is particularly pronounced in international cases, which typically require significant travel and cross-border coordination.

Aisling O'Sullivan

O'Sullivan: The COVID-19 pandemic (and government responses to the crisis) has provided fertile ground for fraud and illegal profiteering across all industry sectors. Throughout the UK lockdowns, there has been a constantly evolving landscape of frauds committed by those seeking to take advantage of the uncertainty that the pandemic has created. For example, the financial services sector reported the emergence of COVID-related ecommerce frauds involving fake or non-existent hand sanitiser or PPE. In addition, new forms of COVID-related cyber-fraud have highlighted how rapidly investigators and practitioners are required to grapple with new fraud mechanisms and adapt traditional defence and investigative measures.

More generally, as enforcement agencies adapt and prioritise remote and safe working, the rate and speed of investigations has notably decreased. Examples include delays to investigative requests, court closures, restricted access to remote evidence due to information security protocols, technological issues and restrictions on in-person meetings, all of which serve to delay the administration of justice.

"With respect to corporate investigations, work-from-home restrictions, employee furloughs, and diminishing resources have strained the abilities of companies to comply with subpoenas."
- Kevin Sweeney -

Q5. What new challenges have emerged as a result of the shift towards remote working and what steps should companies take to remediate these risks?


James Garrett

Garrett: Some estimates are that 40% of the workforce is currently working remotely, with that number increasing over the next three to five years. Regardless whether the trend will increase or recede, the fact is that having large numbers of employees working remotely creates both management and oversight challenges for companies. One obvious challenge is the ability to maintain visibility into the day-to-day activities of employees – in part to maintain productivity and ensure job performance, but also to verify compliance with policies/procedures and reduce the potential for fraud and abuse.

In many cases, management's connectivity to remote employees is via telephone or, in some cases, video conferencing, but those modes of communication can easily be manipulated by employees that may be intent on committing bad acts. Data privacy and integrity is a significant area of exposure for companies. To the extent practicable, companies should create internal governance mechanisms and a regular cadence of communication that reduces the "idle hands" of employees. Bi-weekly calls or the occasional in-person visit (to the extent possible and taking the necessary precautions to ensure health and safety) can be effective in keeping remote employees engaged and reduce the risk of improper activities.


Neil Keenan

Keenan: The pandemic and new working environment that the majority of us are working in has challenged all of us in many ways, including a heightened risk of fraud. As many of you will be aware, studies of those engaged in fraud have identified three common factors: motive, opportunity and rationalisation. The pandemic and remote working has increased all three factors.

Motive: Many individuals have experienced a reduction in earnings, seen colleagues furloughed or let go, and witnessed a significant impact to the economy and communities in which we live. All of this has not been caused by the actions of the individual or company that employs him or her. These factors have created a motive for a potential fraudster to engage in misconduct.

Opportunity: Working from home has changed the way that controls operate, interactions and communications are made and required the introduction of new technologies and processes. In addition, we have witnessed job reductions and revised responsibilities. Uncertainty and change provides the perfect conditions for fraud to occur, where oversight may have diminished, responsibilities are misaligned, and training staff in new areas of responsibility or changes in processes is less effective.

Rationalisation: Fraudsters can rationalise their behaviours in such an environment on the grounds that "this is to safeguard my family," "this will assist the company survive," "this is not my fault and I should not be the one to suffer" etc. The list of 'excuses' could be almost endless.

In light of this environment, companies need to be vigilant and go back to the cornerstone of a robust compliance programme. Senior leadership need to reinforce that the company will continue to operate in an ethical and transparent manner. Communications should be frequent and transparent to diminish uncertainty, provide training and continue to make employees feel connected to the company and its values. Training on new policies, procedures and technologies needs to be effective and frequent, with employees aware of any new roles and areas of responsibility. Companies that make their employees feel connected to the business and invested in its future success, will significantly deter anyone tempted to engage in misconduct.


Aisling O'Sullivan

O'Sullivan: Data security has presented the biggest challenge for 2021 as a large proportion of the UK's workforce continue to work remotely.

Individual risk: More than ever before, people are relying on their home broadband and home computers for remote working. Employees using home broadband, as opposed to safer office networks, expose themselves to the risk of hackers exploiting those less robust connections. In addition, there is increased adoption and deployment of cloud facilities by companies, so that employees can access the computing infrastructures, platforms and services they need. Companies therefore need to ensure that their cloud storage is secure and meets necessary regulations to protect the company itself and the data in question. Organisations also need to ensure that they have a comprehensive IT policy and that employees are aware of the same.

Compliance and regulation risk: Companies need to be aware of the local legislation that applies to them and advise their employees accordingly. For example, are employees correctly moving data in compliance with the relevant data regulation/legislation?

Physical risk: Being away from secure office locations also opens several physical risks. Virtual assistant artificial intelligence (AI) technology devices, routers and other internet technology in the home could present data protection risks for any company. As an example, people working in the legal profession in Ireland have been told not to conduct work-related calls when near virtual assistant AI technology devices, for fear of privacy and data breaches as a result of devices recording information.[1]

Another risk to consider when working from home is who else may be privy to confidential firm information. While employees trust their family members, data handled must remain confidential and firms need to be sure that their employees are working in a secure and confidential way that protects the data they are handling.

1. https://www.lawsociety.ie/gazette/top-stories/big-firm-bans-remote-working-staff-from-having-alexa-in-room/

Q6. Can you outline the best practice for corporate governance and internal control considerations?


Dennis Miralis

Miralis: Corporate governance and internal control considerations are especially pertinent to the developing efforts in Australia to combat foreign bribery. Many Australian companies operate across the globe with varying levels of corruption and bribery risks in each country. The Australian Trade Commission released a practical guide in September 2018 for Australian businesses in managing risks of bribery and corruption. For successful anti-bribery and corruption management, they recommend affirming commitment from the senior management of the organisation, having awareness and detailed policy to account for potential risks, training staff to deal with practical scenarios, incentivising ethical behaviour through promotion and reward of good behaviour, making use of independent legal advice and external bodies, and keeping processes under regular review.

An effective compliance monitoring programme should consider the nature of the organisation, see whether its processes are successful in preventing misconduct, be fast and accurate in detecting offending behaviour, and comply with all applicable laws and regulations. Above all, it is essential that good governance permeates the whole of a business organisation in order to develop a genuinely ethical culture within an organisation. This requires leadership and a commitment to on-going staff training and mentoring that often goes much further than merely formulating anti-bribery compliance programmes. Companies that succeed in fostering a genuine culture of good governance will significantly reduce the reputational risks that come with being investigated including the possibilities of significant penalties.

Q6. Can you outline the best practice for corporate governance and internal control considerations?


James Garrett

Garrett: There is no one-size-fits all to corporate governance and internal controls – they should be tailored to the business and corporate structure of the entity in order to be the most effective. Case in point, best practice is to have clearly defined and easy to understand policies and procedures that protect against fraud and abuse. Further, the best policies and procedures are detailed and, in many cases, lengthy and somewhat complicated given overlapping rules and regulations (e.g., UK Bribery Act and the FCPA or the California CCPA and GDPR).

Indeed, even the best drafting cannot reduce some corporate policies to one to two pages that are easy to understand and comprehend for the average employee. Further, not all policies need to apply to all employees, or only certain aspects of policies apply to certain employees depending on the jurisdiction or their job function. The important thing – and ultimately the best practice – is to have policies and procedures that employees understand and follow – not just that you have them. Depending on the size of the company, that may mean having fewer policies that are narrowly tailored to the company's business or culture, but that are fully understood and become part of the daily activities of employees. Said another way, the "gold standard" of having a true culture of integrity at a company sometimes requires pairing back on policies that might otherwise be "best practice".


Ian Herbert

Herbert: What I would like to do is highlight an interesting development at the SEC involving internal controls cases. In November 2020, two SEC commissioners wrote a dissent in the Andeavor LLC settlement criticising the majority's broad view of Securities Exchange Act Section 13(b)(2)(B), which requires U.S. issuers to maintain a system of internal accounting controls.

Andeavor settled with the SEC for what sounded like an insider trading problem: engaging in share repurchases while in possession of material non-public information. But the SEC did not settle the case for insider trading. Instead, Andeavor was charged with failing to have inadequate internal controls to prevent the improper share repurchases. The dissenting commissioners noted that the statute only governs a company's internal accounting controls, not all internal controls. They criticised the recent trend of using Section 13(b)(2)(B) to require companies to adopt all worthy policies and procedures related to good corporate governance, regardless of their connection to the company's accounting.

To be clear, this is a dissent and isn't yet the majority view, but it is something that we are watching closely. We think these dissenters are right on the law and would not be surprised to see a company take this issue to court in the coming years.


Arantxa Geijo Jimenez

Jiménez: The starting point is to formulate a compliance programme that is tailored to the firm's/company's characteristics, such as size, operations, and geographical presence. The compliance programme must, of course, comply with and address national and international governing laws.

The importance of having a robust compliance programme cannot be overstated. In addition to deterring wrongdoing by an entity's internal and external workforce, having a solid compliance programme in place can act as a defence against a company's alleged criminal liability. For instance, Article 31bis.2 of the Spanish Penal Code provides that an entity can be exempted from criminal liability if, prior to the commission of the crime, it adopted and implemented an effective compliance programme, along with the other conditions established therein. Article 31bis.5 of the Spanish Penal Code sets out the requirements that a compliance programme must meet to be effective.

Spain is by no means the only country whose legal regime provides for such a defence. Indeed, in the UK and the U.S. this is known as the adequate procedures defence. In several countries, the establishment of an effective compliance programme that meets national minimum requirements can exempt a company from criminal liability, and/or act as a mitigating factor.

This, of course, is not a novel suggestion, as many countries already require that companies institute a compliance programme to comply with anti-money laundering regulations.

Nonetheless, a simple box-ticking exercise is not enough. Instead, in order to establish a solid corporate governance framework, it essential that a company's management instils a culture of integrity. This can be achieved through, for instance:

- Clear communication from the top as to what actions will not be tolerated, as well as the consequences for employees who commit such actions;
- Clear communication from the top that encourages whistleblowers to come forward without fear of adverse consequences;
- A whistleblower system that protects the anonymity of whistleblowers – this requires strong internal controls to protect their identity; and
- Training programmes for employees.


Neil Keenan

Keenan: It is easy for companies to be very internally focused, which is understandable considering the workload of often under-staffed or -supported compliance and internal audit teams. However, there is significant merit in observing market trends, enforcement actions and the opinions and observations of other market participants.

Many significant corporate scandals often come from sources outside the company. For example, the stock option investigations that impacted tech companies in the early 2000s originated from an academic study that identified the correlation of stock grants at the time of 'troughs' in the company's share price. Similarly, the SEC's EPS Initiative mentioned in this discussion, also originated from academic circles who identified an under-representation of the number four in the first post-decimal digit of EPS, essentially implying there is an incentive for management to "round up" EPS results to manage "street" earning expectations. In 2020, we witnessed the significant accounting scandal at Wirecard that was initially unearthed by financial press who highlighted anomalies in previous reports and public statements. Also in 2020, short seller reports brought to light the now reported frauds occurring at NMC Health and Finablr, both London Stock Exchange listed companies.

When reading such reports, studies or articles, it would be easy to say "this could not happen to us." Instead, I think it prudent for companies and their boards to look internally for indicators of similar misconduct occurring within their operations and assess if existing internal controls would prevent or detect such misconduct. Rather than re-run the annual risk assessment as it has been done for the past number of years, companies could benefit from an alternative approach. Look at publicly reported enforcement trends noted in their industry or the geographies in which they operate, and go through the exercise of understanding and being able to demonstrate that such risks would not apply or are adequately mitigated within their own organisation. This would not only enhance the risk assessment process, but also provide excellent training examples for management, potentially asking them to assess risks differently through the lens of actual events, not abstract or generic scenarios.

Q6. Can you outline the best practice for corporate governance and internal control considerations?


Hidetaka Miyake

Miyake: Some hotly discussed topics regarding the corporate governance of listed companies in Japan include the expected roles and qualifications, and the appropriate number of outside directors in order for the board of directors of a company to effectively supervise the management's execution of the company's business. Recent amendments to the Companies Act have made it legally necessary for certain companies to have at least one outside director. Appropriate governance systems vary from company to company, but it has been argued recently that for a high level of governance, at least one-third or a majority of the board of directors should consist of independent outside directors.

Another widely discussed topic relates to the internal controls of listed companies. Even if a company has well-designed policies and procedures in place, there are still cases where the operation of such policies and procedures is not conducted thoroughly and instead becomes a mere formality. Therefore, attention has recently been focused on the status of the operation of internal controls. In order to enable the continuous operation of internal controls, it is important to apply the PDCA (Plan-Do-Check-Act) cycle, in which the internal audit function plays a vital role by finding vulnerabilities and recommending remedial measures to address them.

In Japan, there are not many professional internal auditors in the market, and even in most listed companies, the resources for the internal audit function are insufficient. As a best practice, however, it would be desirable for a company to establish an internal audit department with a sufficient number of internal auditors with the requisite knowledge and experience.

Q7. What steps should a company should take upon discovering fraud?


James Garrett

Garrett: The most important step a company should take once relevant evidence has been secured is to do a thorough and complete investigation to understand what transpired and discover the root of the cause. Too often, the facts seem clear and relatively simple and the investigation is concluded too early. In some cases, the facts may be straightforward, but the root cause of the fraud may run much deeper. In such cases, the actions taken in response to the fraud may address the issue at hand, but they will have little impact on whatever caused or created the opportunity for the fraud in the first place. One way to avoid such a result is to engage a third-party to participate in the investigation or double check the work performed by the internal team. By asking questions and not knowing all the facts, oftentimes a third-party can see things that the internal team might have missed or didn't acknowledge in conducting the investigation.


Ian Herbert

Herbert: The first step is to make sure you stop the fraud. Take steps to ensure that whatever potential problems you have uncovered are not allowed to continue. Apply a tourniquet to the wound and stop the bleeding. After that initial triage, you can scope your investigation to determine the nature and magnitude of the fraud, what the company can do to prevent similar issues in the future, and whether and how to interact with regulators.

Part of the scoping exercise will be determining who should conduct the investigation: internal resources such as compliance, legal, or HR; an outside law firm; or an outside law firm under the guidance of the Board of Directors or an independent committee. Whether to use outside counsel will depend on a number of factors that are specific to the incident and the company, but some factors to consider are: the significance of the potential liability and whether the conduct is potentially criminal; the likelihood of disclosure to government agencies; the resources that an investigation will take and whether those resources are available in-house, privilege considerations, and any specialised skills, such as language fluency.

When subjects of the investigation are senior management or in the chain of command for compliance or legal, or when there is a significant public relations risk that could require the need to demonstrate an independent investigation, you may want to consider having outside counsel directed by the board of directors or an independent committee. In addition, if there are potential auditor issues, which is increasingly common, you will likely want to engage outside counsel to assist with those issues as well.

Another part of the scoping process will be to consider how broad the investigation needs to be. If you hire outside counsel, you will want to have a conversation with them about this. If you are doing the investigation internally, it is ok to keep the investigation narrowly tailored if that is what the facts justify, but despite the fact that some regulators have said that companies don't need to boil the ocean for every instance of wrongdoing, scope is one of the issues on which companies are routinely second-guessed. You want to ensure that you get to the truth, but it can be ok to do so without excessively disrupting the business.

Whatever decision you make about the scope of the investigation, make sure you document the decision. Particularly at the start of the investigation, things move very fast and you will know just a small fraction of the facts. It is important to document your rationale at the time so that you aren't later blamed for taking a different approach from an ex poste posture. This is just the tip of the iceberg. There are also document preservation issues to consider right at the beginning of the investigation, for example, but this discussion about scoping is an important first step.


Arantxa Geijo Jimenez

Jiménez: There are two key elements to address in these cases: (i) whether there is an effective fraud prevention programme; and (ii) reporting the crime to the competent authorities. Thus, under Spanish law, a programme that includes appropriate monitoring measures to prevent the commission of fraud exempts a legal entity from criminal liability (Arts. 31bis 2 and 4 of the Spanish Penal Code). In addition, reporting the offense and collaborating with the authorities in the investigation may mitigate the penalty to a company.

Consequently, as a precautionary measure, it is advisable that a company formulates a fraud risk management strategy. This includes putting in place a response plan, in the event that fraud is discovered, which clearly sets out the steps to be taken. Such a response plan should include the company's policy and zero-tolerance stance towards fraud, a definition of what constitutes fraud, allocation of responsibility and procedures with regard to clear reporting of a suspected fraud, and collection and preservation of evidence.

Moreover, there are a few key steps that a company should take upon any allegation of fraud. Firstly, it is imperative that a member of senior management be appointed as responsible for handling the case. It is also recommended that an internal team be assembled. It is vital that internal conversations are kept confidential. This is to avoid tipping off the suspect, who may in turn destroy evidence and thereby hinder a future investigation. The internal team, depending on the extent and complexity of the fraud, should assess whether it is necessary to appoint an external investigation team. This may be needed especially if proper investigation requires specialised expertise. Lastly, as soon as the suspicion of fraud arises, it is essential to collect and preserve potential evidence, all the while making sure that it is not altered in any way. Details of the alleged fraud should be recorded and documented.

Finally, it is also essential that the programme be reviewed in order to identify and strengthen the weaknesses of the programme that enabled the commission to the criminal offence. Under Article 31 quarter d) of the Spanish Penal Code, if these measures are taken before the trial takes place, it will serve as a mitigating circumstance.

Q7. What steps should a company should take upon discovering fraud?


Neil Keenan

Keenan: Studies have shown that the most common means of detecting fraud is through a whistleblower report. When such a report comes in, very often anonymous, the initial reaction of many company officers is to take steps to try and identify the individual making the complaint. This can be a fundamental error when a fraud scheme is initially detected. Firstly, trying to pursue the identity of the whistleblower can appear to be an attempt to discredit them or the misconduct they are reporting, and could open the company up to claims of retaliation. Secondly, and equally important, this can prohibit an objective evaluation of the allegations set forth in a whistleblower report. Compliance Officers and legal counsel should ask themselves if the alleged misconduct has occurred previously, been identified in risk assessments, and poses a genuine threat to the business (i.e., are there possible motivations and opportunities for someone to engage in such conduct?).

While there is clearly a need to assess the accuracy of whistleblower reports, I recommend that this be done through an assessment of the "facts" as stated in the report, and assess any potential benefits for someone to engage in such alleged misconduct. This evaluation should not be done with the mindset of understanding the motivation of the whistleblower bringing the complaint forward. I then recommend that companies use analytical approaches to identify if the alleged events or transactions could have occurred. This can be achieved through a review of relevant corporate records, based on the individual allegations, but can include: financial reports, bid files, commission payments, contract awards, management accounts (budgets vs. actual results). Such an analysis may highlight possible motivations for those involved, identify areas of immediate attention to focus the investigation, point to relevant data sources and others who may have knowledge or relevant information. Such factors will permit an early case evaluation that, on completion, permits the company to assess the potential merits of the whistleblower report, its potential severity and whether outside advisors are needed to support the upcoming investigation.


Kevin Sweeney

Sweeney: At the first reliable indication of fraud, the company should retain outside legal counsel to conduct the investigation. Under U.S. law, communications with counsel generally are protected by privilege, while communications with company personnel are not. The use of outside counsel also serves to protect the information learned during the investigation from discovery by third-parties and lessens the possibility of misunderstandings among employees/witnesses about their relationship to the investigating attorney. Counsel should assure that the company discretely secures and preserves all potential evidence known to it.

To the extent forensic consultants are necessary, they should be hired by outside counsel rather than the company itself, which can cloak communications and analysis with the attorney-client and work product privileges of counsel. Although appropriate in some cases, using in-house personnel could subject the information learned during the investigation to discovery and may actually generate a whistleblower claim by the employees involved.


Aisling O'Sullivan

O'Sullivan: (i) Document the date, time, and other details related to the initial discovery: This is key information that will inform any subsequent investigation, disciplinary/termination proceedings and/or insurance claims.

(ii) Maintain confidentiality: Do not confront the potential suspect. Only inform individuals who need to know about the discovery.

(iii) Safeguard potential evidence: Preservation of evidence is key. Companies should secure all potential evidence. Electronic evidence is fragile and easily altered and therefore companies should ensure that computers, company mobile phones and external electronic media sources (such as USB drives) are seized. Maintaining the evidence will greatly assist any subsequent investigation.

(iv) Deal with the suspected employee/s (if required): Don't terminate the suspected employee's employment immediately as this could cause difficulties for the evidence gathering process. Instead, companies should restrict a suspected employee's access to company data and should take steps to seize any company devices documents from them. Companies should also seek employment law advice to ensure that they do not infringe suspected employees' rights.

(v) Gather an investigation team: Companies should appoint a team of core personnel to deal with the discovery. Knowledge of the discovery should be confined to this team unless required otherwise by law. Companies should also consider whether they need to enlist the services of a forensic accountant, a computer forensic specialist, and/or investigator. Best practice dictates that any experts hired are external as using in-house might create questions as to their objectiveness during the investigation. Companies should also instruct external lawyers who can guide them through any investigation process.

(vi) Notify insurance provider: Companies must notify their insurance providers of the fact of discovery of fraud within 30 to 60 days, depending on the specific policy. Failure to do so could cause a loss of coverage. Companies will also need to document any losses with their insurance provider within a specified timeframe.


Hidetaka Miyake

Miyake: When fraud is detected in a Japanese listed company's organisation, the company should implement crisis management measures in order to minimise damage to its corporate value and reputation.

The first step in crisis management is to find the relevant facts, and companies normally conduct fact-finding investigations through interviews with officers, employees and third parties involved in the alleged fraud, and (if necessary) conduct digital forensics to review relevant emails and other electronic data.

Based on facts found in the investigation, the next step is to analyse the cause of the fraud, introduce measures to prevent the recurrence of the same type of fraud, and consider disciplinary actions against the persons involved. The analysis of the causes of the fraud has recently become a particularly important step in implementing crisis management practices in Japan. This is because the regulators and stock exchanges have the view that the same type of fraud can happen again if companies fail to find the "root cause" and implement effective preventative measures to address it. These root causes often include corporate culture and governance issues.

Q8. What advice would you give to clients involved in cross-border investigations?


Dennis Miralis

Miralis: Clients should be advised that an effective cross border legal strategy requires consideration to how to deal with parallel investigations, whether by regulators or law enforcement, in multiple jurisdictions. This requires the capacity to critically think as an "internationalist" when providing legal advice and the ability to consider strategies and solutions that do not expose the clients to lengthy protracted litigation across the globe, if feasible.

Identifying strategic partners in each of the implicated jurisdictions is essential, as the overall strategy will need to be a team effort, even if one jurisdiction may take more of a leadership role in coordinating and allocating the tasks that need to be undertaken.

Clients need to remain focused on properly assessing the key risks and dealing with those in such a way that the balance of the legal problems, across the remaining jurisdictions, can be resolved at the same time, if possible. This requires the ability to also bring regulators and law enforcement officials from multiple states into the negotiations on a common understanding of how the matters may be resolved. These investigations by their nature are very complex and may take several years to be completed.

Q8. What advice would you give to clients involved in cross-border investigations?


James Garrett

Garrett: It is extremely important to understand and appreciate the cultural differences that are associated with nearly all cross-border investigations. The same is true for language-related differences. What is "normal" in one jurisdiction may be "not normal" or even inappropriate in another, but the analysis does not stop there.

Interpretation and compliance with policies and procedures is greatly impacted by the cultural lens that people look through and that lens is further distorted by language. As such, corporate policies and procedures should be tailored to employees in different countries wherever possible, and they should be in the local language to the extent practicable. English may be the official language of a country, but that does not mean that it is an employee's native language or that the American English used is understandable (or the inherent nuances in the policy understood) to someone who learned English as an adult or does not speak English on a regular basis.

All of these factors need to be taken into consideration when conducting a cross-border investigation and trying to get at the facts and root cause of the alleged fraud.


Ian Herbert

Herbert: There has been a significant increase in cross-border cooperation from regulators around the globe. The Goldman resolution, which I mentioned earlier, is an example of that, with fines going to U.S. federal and state agencies, as well as regulators in the UK, Singapore, and Hong Kong. Many clients care less about who they are required to pay and more about the total amount. Coordinating with multiple authorities across multiple jurisdictions is a daunting task, but essential in order to ensure getting credit in one jurisdiction for payments made in another. Such coordination requires a team that is working together.

One aspect of an investigation that is always important but becomes significantly more important – and difficult – in a cross-border investigation is the concept of attorney-client privilege. Privilege in the UK is much more limited than in the U.S., particularly in connection with company investigations. For example, in the U.S., communications between in-house lawyers and employees can be privileged whereas that is quite rare in the UK and EU. But on the other hand, the U.S. regulators generally don't recognise the idea of limited waiver, which is more common in the UK, and the U.S. regulators will expect that documents provided to other regulators are provided to the U.S. government.


Arantxa Geijo Jimenez

Jiménez: Cross-border investigations have become increasingly common. This is due to both globalisation and regulators' focus on tackling financial crime, which in most cases involves multiple jurisdictions. In addition, the entry into force of whistleblower protection laws, especially throughout the past two decades, has also been a contributing factor to the surge of cross-border investigations.

The key point is the coordination and common strategy adopted throughout the different jurisdictions. Cross-border investigations are often complex largely because they involve different jurisdictions, legal systems, languages, cultures and local laws. Whether a cross-border investigation is triggered by an internal allegation or finding, or by a regulatory authority's notification, there are a number of factors that should be considered.

Given the multijurisdictional nature of cross-border investigations, local counsel or specialists are usually needed. In the absence of local in-house counsel, hiring of local experts is usually recommended. This is because the legal requirements of each jurisdiction involved in the investigation must be observed and the violation thereof might not only compromise the validity of the investigation altogether but may also give rise to criminal and/or civil liability.

In this regard, careful attention must be paid to areas such as data privacy, blocking statutes, attorney-client privilege and disclosure requirements, especially to regulatory authorities. Data privacy laws and blocking statutes can be particularly problematic. Indeed, data privacy legislation may prevent counsel from questioning employees and accessing a broad range of individual data. Moreover, blocking statutes prohibit the transfer of certain type of documents and information to a third country.

It is also important that a company appoints an appropriate internal investigation committee to oversee the investigation. The internal investigation committee should liaise with outside counsel, who should, in turn, lead and manage the cross-border investigation.


Kevin Sweeney

Sweeney: My advice would be to ensure that the company and its representatives work closely together to set forth a defined work plan at the very start of any cross-border investigation. The work plan should define the subject matter and scope of review and lay out the details of what is to be accomplished to include the parameters of document collection and interviews. In tailoring such a plan, the investigative team should assess the risks to the client, the origin of the issue, foreign law concerns, and anticipate the scope and focus of government inquiries.

Moreover, it should be realistic about the possibility that investigative plans often change and should therefore build in commensurate flexibility. Taking time at the beginning of a cross-border investigation to craft a well-thought out plan can pay big dividends in aligning expectations and fostering confidence in the collective path to resolution.


Aisling O'Sullivan

O'Sullivan: Retain local counsel/experts: Companies involved in cross-border investigations are faced with navigating a variety of foreign laws and regulations that, in many respects, change the way an investigation can be conducted. Foreign data privacy laws and regulations pose some of the greatest challenges to conducting cross-border investigations because of restrictions on the types of data that can be collected and transferred out of the jurisdiction. For example, China has strict laws that prohibit the collection, review, and transfer of "state secrets" and other information that is in China's national interest. However, China's laws do not define what are state secrets or national interests. It is therefore imperative to engage local experts are who are familiar with making this assessment and navigating these risks. Similarly, if an investigation entails the conduct of employee interviews, local labour laws should be consulted.

Proactively identify and address cultural differences: Cultural differences underlie cross-border investigations and can create significant problems if investigators do not understand and respect these differences. What may be acceptable to say or do in one culture may offend someone from another culture.

Consider issues of admissibility of evidence throughout: Companies should consider which, if any, jurisdiction will prosecute any offences uncovered during an investigation, and the relevant rules of admissibility. For example, in *United States v. Allen* (No. 16-898 (2d Cir. 2017)), a U.S. court held that because the defendants' testimony was compelled by UK law, the government's use of it in securing an indictment and at the trial of the defendant violated their Fifth Amendment right against self-incrimination.

Carefully consider privilege: Differing concepts of privilege create challenges for corporates subject to cross-border investigations or litigation. The fact that a document enjoys a privileged status in one jurisdiction is no guarantee that it will be afforded that protection in another. Companies should therefore seek local legal advice on the rules on privilege and disclosure in each of the relevant jurisdictions.

In addition, companies should be mindful of the different privilege rules that apply to individual members of a global investigation team. It may be advisable to limit creation of and/or access to particular classes of documents by individuals based in jurisdictions where those documents are vulnerable to disclosure.

Q8. What advice would you give to clients involved in cross-border investigations?


Hidetaka Miyake

Miyake: There is no attorney-client privilege under Japanese law. Therefore, it is important to advise Japanese companies involved in cross-border investigation cases of this issue, particularly taking into account the protection of attorney-client privilege in foreign jurisdictions.

In Japan, upon the discovery of an allegation of serious fraud, it is common practice for a company to establish an independent investigation committee (often called a "third-party committee" (*daisansha-iinkai*)) composed solely of outside experts who have no interest in the company and who are therefore free from conflicts of interest. The investigation report of the third-party committee is also often made public to investors and other stakeholders. The practice of establishing third-party committees is a development that is particular to Japan due to the unique circumstances of Japanese companies in which many directors concurrently manage business operations and the board of directors is not highly independent from the management.

In cross-border investigation cases in which a third-party committee is established in Japan, there may be a conflict between accountability to stakeholders in Japan and protection of attorney-client privilege in foreign jurisdictions. If all or part of an investigation report is not disclosed to the public with an emphasis on the protection of attorney-client privilege, it would be advisable for the company to publish a press release fully explaining to stakeholders the reasons for taking such measures.

Q9. What are the key advantages and disadvantages of a Deferred Prosecution Agreement ("DPA")?


Dennis Miralis

Miralis: A DPA is an agreement negotiated between a prosecutor and a corporate defendant, similar in nature to a plea deal. It is offered at the discretion of the prosecution and involves a deferral of prosecution in exchange for compliance with terms such as admission of facts, cooperation in an investigation, or payment of a penalty. If the DPA is breached, the prosecution can reopen and proceed with the case.

There are many advantages of a DPA. Corporate crime can be difficult to detect or establish without inside information, with offenders able to obscure their own activity. DPAs provide an avenue for such information to be provided to prosecutors. Compensation for victims of corporate crime is facilitated through a guaranteed payment of fines through the DPA process, avoiding lengthy court proceedings with uncertain outcomes. This also has the advantage of saving Government funds and resources. Incentive is also created for companies to self-report wrongdoing in order to avoid prosecution.

The main disadvantage of a DPA is reducing the deterrent for criminal behaviour. Large companies may commit crimes knowing they are likely to go through a DPA scheme, seeing this as a business cost rather than a penalty. It could be seen as inequitable for corporations to have access to DPAs whereas individuals in a similar situation would not have the same opportunity to avoid prosecution. There may also be insufficient incentive to encourage self-reporting without a guarantee of a DPA in proceedings.


Aisling O'Sullivan

O'Sullivan: Key advantages:

- DPAs can bring a swifter end to an investigation and minimise reputational and economic losses caused by the uncertainty of the outcome of a prosecution.
- Improving the ability of law enforcement agencies to identify and prove corporate crimes, from information provided during the DPA process.
- Ensures fines are commensurate with companies turnover/resources. DPAs ensure that shareholders, suppliers, employees and business partners are not unduly punished for the actions of a few.
- Facilitating faster compensation for victims of corporate crimes.
- Saving government funds and resources by avoiding lengthy and protracted legal proceedings which means government resources are free to focus on more egregious wrongdoing.
- Encouraging companies to self-report to avoid prosecution may prompt companies to improve their internal protection for whistleblowers.

Key disadvantages:

- Potentially onerous conditions imposed on a company as part of an agreement. A failure to adhere to those conditions may result in a prosecution being resumed.
- The availability of DPAs might encourage high net worth individuals and companies to commit crimes knowing that they will likely be offered a DPA. In short, the resulting fines might be perceived as just the cost of doing business.
- The unavailability of DPAs for individuals may be seen as inequitable. One rule for those with resources, and one for others. There is currently insufficient incentive to guarantee self-reporting, particularly as the decision to offer a DPA remains at the discretion of the prosecutor. The uncertainty may serve to discourage corporates and individuals coming forward.


Hidetaka Miyake

Miyake: There is no concept of DPA under Japanese law. However, the so-called Japanese version of the "plea bargaining" system was introduced in June 2018. This new plea bargaining system made it possible for companies suspected of committing certain types of corporate crimes to conclude their cases without prosecution by entering into an agreement with the public prosecutor. In order to take advantage of this system, however, companies must cooperate in the investigation and trial of the criminal cases of certain other person(s) in accordance with the terms and conditions set out in the agreement with the prosecutor. A typical case where a company may use this system is where the company agrees to cooperate with the public prosecutor in the investigation and/or trial of the criminal cases of its officers and employees.

The advantage of this type of plea bargain is that companies can avoid criminal penalties and other penalties such as being disqualified from bidding for government projects. On the other hand, in the case of Japanese companies, there is a risk that their reputation may be damaged by giving the impression to the public that they have sacrificed their officers and employees in order to protect the organisation. Such reputational risks should be taken into account especially in cases where officers and employees have colluded in cartels or committed bid-rigging or bribery for the benefit of the company and not for their own benefit. In order to reduce these risks, it is important to establish and thoroughly implement a corporate policy that emphasises compliance rather than profits.

Q10. What impact, if any, will Brexit have on UK and European fraud & white collar crime efforts?

Arantxa Geijo Jimenez

Jiménez: Law enforcement and judicial cooperation in criminal matters will be seriously impacted by Brexit. Both the UK and EU perceive this issue as a priority area, as demonstrated by Part III of the Political Declaration agreed to by both parties, which states that "[t]he future relationship will provide for comprehensive, close, balanced and reciprocal law enforcement and judicial cooperation in criminal matters, with the view to delivering strong operational capabilities for the purposes of the prevention, investigation, detection and prosecution of criminal offences."

In terms of anti-money laundering regulation, Brexit is not likely to have a significant impact. International anti-money laundering standards are set by the Financial Action Task Force (FATF), of which both the UK and the European Commission are members. The UK has already transposed the EU's most recent money laundering directive, nicknamed the Fifth Money Laundering Directive, into its national legislation through the Money Laundering and Terrorist Financing Regulations 2019, which will remain in force after Brexit.

The EU is currently working on a sixth Directive which the UK will not be obliged to implement nationally. Nonetheless, with both the EU and the UK complying with FATF standards and recommendations, regulatory divergence in this area is unlikely to arise. Indeed, the Political Declaration, which sets out the framework for the future relationship between the UK and the EU, explicitly states that the "Parties agree to support international efforts to prevent and fight against money laundering and terrorist financing, particularly through compliance with [FATF] standards and associated cooperation".

In addition, other areas, such as bribery and fraud, are already covered by UK domestic statutory regimes, namely the UK Bribery Act 2010 and the UK Fraud Act 2006.