CorporateLiveWire

FRAUD & WHITE COLLAR CRIME 2019

VIRTUAL ROUND TABLE

www.corporatelivewire.com

Introduction & Contents

In this roundtable the panel of seven experts in fraud & white collar crime discuss the latest regulatory changes and interesting developments on a local, regional and global scale. We discover which fraud & white collar crime trends prosecutors will focus on in 2019 whilst also addressing other prevalent topics such as whistleblowing & self-reporting incentives, the impact of smart technology, and a summary of recent noteworthy case studies. Featured countries are: Australia, Cayman Islands, Germany, Turkey, United Kingdom, and the United States.

James Drakeford
Editor In Chief

5 Q1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

10 Q2. What international conventions apply in your jurisdiction?

11 Q3. Can you outline the key fraud and white collar crime trends?

13 Q4. Have there been any recent regulatory changes or interesting developments?

16 Q5. How is the continuous development of smart technology impacting fraud and white collar crime?

18 Q6. Have there been any noteworthy case studies or examples of new case law precedent?

21 Q7. What is the difference between unlawful and unethical conduct and to what extent has the line become increasingly blurred in recent years?

22 Q8. At what point does liability shift between employee and employer? And what measures should businesses incorporate to counteract the increasing regulatory compliance burden?

23 Q9. How can companies ensure they get the balance right between implementing risk management and risk prevention?

24 Q10. Can you talk us through the various steps a company should take upon discovering fraud?

27 Q11. To what extent has whistleblowing and self-reporting incentives changed the way companies manage and respond to fraud?

28 Q12. What options exist for companies to investigate the fraud and recover the proceeds in cross-border fraud or misconduct?

30 Q13. In an ideal world what would you like to see implemented or changed?

Meet The Experts

Jodi L. Avergun - Cadwalader, Wickersham & Taft LLP
T: +1 202 862 2456
E: jodi.avergun@cwt.com

Jodi Avergun represents corporations and individuals in criminal and regulatory matters involving, among other things, the FCPA, securities enforcement, health care, and general white collar matters. Jodi has successfully represented both companies and senior executives in internal investigations, matters before regulatory bodies including the SEC and the DEA, and in civil and criminal matters in federal court. She has also designed and implemented compliance programs for many clients. Before joining Cadwalader, Jodi served in numerous capacities in the DOJ, including as chief of staff of the DEA, and as an Assistant U.S. Attorney in the Eastern District of New York.

Esra Bicen - EB Legal
T: +90 212 283 00 53
E: ebicen@eblegal.net

Professor Bicen has twenty years of experience as a litigation and transaction lawyer in Turkey and in the United States. Her practice, lectures and publications focus on corporate, commercial (gaming, fintech, healthcare) and financial compliance, ISDA, EPC, procurement contracts and international arbitration. From 1997 to 2000, she practised with a leading Istanbul law firm specialising in international investments, cross-border financings, public tenders and dispute resolution. From 2003 to 2007, she practised complex litigation with a leading American law firm involving mass tort actions. Between 2008 and 2011, she served as a General Counsel responsible for Ernst Young Central and Southeast Europe area and co-headed EY's investment consulting firm in Turkey.

In 2011, she was appointed as a part-time faculty member at John F. Kennedy University School of Law while continuing her law practice with a tier-one Istanbul law firm. Since 2015, she maintains her law practice EB LEGAL in Istanbul and Silicon Valley and continues to teach at JFKU School of Law on international contracts and international arbitration.

Craig Weston - Irwin Mitchell LLP
T: +44 (0) 207 421 3976
E: craig.weston@irwinmitchell.com

Craig is a Senior Associate (Employed Barrister) at Irwin Mitchell LLP and is a regulatory and corporate crime lawyer with a particular expertise in advising and defending corporates and individuals under investigation by or being prosecuted by bodies such as the Serious Fraud Office (SFO), the Crown Prosecution Service (CPS), the Financial Conduct Authority (FCA), the Environment Agency and Trading Standards. Craig regularly provides commercially aware advice on issues such as bribery and corruption, modern slavery and corporate criminal liabilities. He is often engaged in enhanced due diligence projects (particularly in the investment and M&A context) and internal investigations.

Tobias Eggers - PARK Wirtschaftsstrafrecht
T: +49 231 9580 68-12
E: eggers@park-wirtschaftsstrafrecht.de

Tobias Eggers focusses on international cases of corruption, anti-trust law and capital market offences. He leads the Compliance department at PARK and has wide experience in advising multinational companies. He serves as an Ombudsman for several corporations.

He is a Certified Lawyer for Criminal Law, teaches criminal law at Osnabrück University and is actively involved in the scientific discussion in his field. Tobias studied Law in Germany and Scotland. When admitted to the bar in 2007 he worked at one of the leading law firms in the Ruhr region. In 2011 he joined PARK and is now one of the partners of the Firm.

Meet The Experts

Salvatore LaScala - Navigant Consulting, Inc.
T: +1 212 554 2611
E: salvatore.lascala@navigant.com

Salvatore LaScala is the managing director and co-lead of Navigant's Global Investigations and Compliance practice in New York, NY.

Possessing a broad range of subject matter knowledge and expertise, Salvatore applies his 20+ years of hands-on experience to conduct investigations and compliance reviews on behalf of financial institution clients responding to regulatory or law enforcement matters concerning anti-money laundering (AML), Bank Secrecy Act (BSA), USA PATRIOT Act and Office of Foreign Assets Control (OFAC).

Salvatore leads large teams that regularly perform historical transaction reviews ("Lookbacks") and Know Your Customer (KYC) / Customer Due Diligence (CDD) / Enhanced Due Diligence (EDD) file remediation work. He also helps clients overcome AML and OFAC backlogs by deploying teams embedded at his clients' work sites to that disposition alerts. Salvatore's expertise also includes assisting clients with the selection, implementation, optimization and validation AML and OFAC compliance technology consulting and enhancing AML transaction monitoring detection scenarios and sanctions filter interdiction logic.

Angela Barkhouse - Krys Global
T: +1 345 815 8422
E: angela.barkhouse@krys-global.com

Angela is the Managing Director in the Cayman Islands office for Krys Global, a financial investigation and asset recovery firm with offices focused in offshore jurisdictions. Angela applies her broad experience in assessing corruption, investigating fraud and winding up entities to derive practical solutions to ascertaining the facts and repatriating stolen assets. Where businesses want to be proactive in risk management, Angela can assist with mitigating the impact of financial crime and economic loss.

With 15 years' professional experience, Angela has consulted with governments, law firms, banks, corporations and NGO's to investigate financial fraud, bribery, corruption, conflicts of interest, embezzlement, stolen sovereign wealth, and make cross-border asset recoveries.

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

Dennis Miralis is a leading Australian defence lawyer who acts and advises in complex domestic and international criminal law matters including:

White collar and corporate crime, Money laundering, Serious fraud

Dennis Miralis specialises in representing clients in transnational /international criminal law matters such as assets forfeiture proceedings involving multiple jurisdictions (including China, Hong Kong, Singapore, South Korea, Russia, the UK, Canada, Europe, the USA and Mexico) as well as the following areas of transnational / international criminal law:

International money laundering law, International Proceeds of Crime law, Bribery and corruption law, Transnational crime law, Cybercrime law, Extradition law, Mutual Assistance in Criminal matters law

He appears in all courts throughout Australia and regularly travels outside of Australia for complex international / transnational criminal law matters.

Q1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

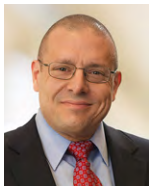
Tobias Eggers

That would be § 263 (fraud by deception) and § 266 (breach of trust) of the German Penal Code. For bribery there are several provisions; most important of which are § 299 (corruption in private sector) and §§ 331ff (corruption in public sector). An area of law that has seen several important changes within the last few years (broader offences, better investigative measures, stronger international teams, focus point in compliance systems).

Insider trading, too, has seen several changes in the last year that derived from EU directives. You will find it in a chain of laws which you will have to read together: § 119 Sub 3 Securities Trading Act which relays to several European directives. The most important one is the EU Market Abuse Directive ((EU) Nr. 596/2014). These offences usually carry a sentence of up to five years imprisonment. In severe cases, fraud can go up to 10 years.

Given that not "what really happened" will make the offence but "what can be proven" the main thing in defence work will usually be managing the flow of information. Information will often be the lever that can make prosecutors budge. Therefore, tip one: Don't give anything unless you get something in return.

Also worth noting: White collar crime cases are often terminated before reaching court. And without anyone going to prison.



Salvatore LaScala

As a general matter, corporate and business fraud includes illegal or unethical conduct that unjustly enriches a company and/or individual. Bribery and corruption and insider trading are examples of such behaviour.

The seminal anti-bribery and corruption regulation in the United States is the Foreign Corrupt Practices Act ("FCPA"). The FCPA, which is administered by the U.S. Department of Justice ("DOJ") and the U.S. Securities and Exchange Commission ("SEC"), at its base makes it unlawful for certain classes of persons and entities to make payments or provide any other items of value to foreign government officials in exchange for obtaining or retaining business. In addition to the FCPA, there are other federal laws — as well as state and local laws in the U.S. — that prohibit bribery and corruption in other contexts. For example, commercial bribery is where one private party bribes another private party to obtain some type of unfair advantage. Another example of bribery is making payments to a political official in exchange for voting in a certain way or promoting certain legislation.

Insider trading, the trading of a public company's stock with access to material non-public information about the company, is prohibited by Rule 10b-5 of the Securities Exchange Act of 1934. Insider trading is also illegal under U.S. mail and wire fraud statutes, as set forth in the United States Code. Insider trading cases are prosecuted by the DOJ and the SEC.

Q1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

Angela Barkhouse

The Cayman Islands Monetary Authority ("CIMA") has responsibility, under the Monetary Authority Law (2018 Revision) for, among other things:

- Supervising financial services business.
- Monitoring compliance with money laundering regulations.
- Co-operating with overseas regulatory authorities.

It can initiate investigative procedures and bring enforcement action against an entity or an individual that is in contravention of the regulatory regime, whether that is related to corporate fraud or insider trading. It also has powers under other laws including:

- Banks and Trust Companies Law (2013 Revision)
- Building Societies Law (2010 Revision)
- Companies Management Law (2003 Revision)
- Cooperative Societies Law (2001 Revision)
- Insurance Law (2010 Revision)
- Money Services Law (2010 Revision)
- Mutual Funds Law (2013 Revision)
- Securities Investment Business Law (2011 Revision)

CIMA is also responsible for the regulation and supervision of financial services in the Cayman Islands. The Securities Investment Business Law (2011 Revision) ("SIBL") creates criminal offences for insider dealing and market abuse. Regulations created under the SIBL include the Conduct of Business Regulations, compliance with which is mandatory for all those licenced under the law. The offences are strict liability, subject to several defences.

The main provisions dealing with criminal fraud are found within the Penal Code (2013 Revision) as amended (Penal Code). The Royal Cayman Islands Police Service ("RCIPS") is the authority charged with the investigation of corporate and business fraud and has a dedicated department known as the Financial Crimes Unit assigned to this task.

Under the Anti-Corruption Law ("ACL") (2018 Revision) the Anti-Corruption Commission ("ACC") can receive, consider and investigate reports to the Commission any corruption offences as set out in the ACL, including the detection and investigation of suspected corruption offences, attempts to commit an offence, or conspiracies to commit an offence.

The ACL came into force on 1 January 2010 with the intent of giving effect to the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, as well as the United Nations Convention Against Corruption. It replaced the provisions relating to anti-corruption and bribery which previously existed under the Penal Code, and provides generally for four categories of corruption offences: Bribery (both domestic and foreign); Fraud on the Government; Abuses of Public or Elected Office; and Secret Commissions. There are also ancillary offences for failure to report an offence.

"The Royal Cayman Islands Police Service ("RCIPS") is the authority charged with the investigation of corporate and business fraud and has a dedicated department known as the Financial Crimes Unit assigned to this task."
- Angela Barkhouse -

Q1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

Craig Weston

(i) Corporate/Business Fraud:

In the UK the main pieces of legislation relating to corporate or business fraud are contained within the Fraud Act 2006. Section 1 creates a general offence of fraud and introduces three ways of committing it set out in Sections 2, 3 and 4: fraud by false representation (Section 2); fraud by failure to disclose information when there is a legal duty to do so (Section 3); and fraud by abuse of position (Section 4). In each case: the defendant's conduct must be dishonest; his/her intention must be to make a gain; or cause a loss or the risk of a loss to another. No gain or loss needs actually to have been made. The maximum sentence is 10 years' imprisonment.

The most often investigated and prosecuted cases in the context of corporate/business fraud are section 2 and in particular section 4. Section 4 applies where a person occupies a position in which he was expected to safeguard, or not to act against, the financial interests of another person; abused that position; dishonestly; intending by that abuse to make a gain/cause a loss. The abuse may consist of an omission rather than an act.

In addition there is an armoury of other offences that may apply, for example theft under section 1 Theft Act 1968, obtaining property by deception, VAT and duty fraud.

(ii) Bribery and Corruption:

The main piece of UK legislation is the UK Bribery Act 2010 which came into force on 11 July 2011. It creates three potential offences against individuals: bribing another person (section 1), being bribed (section 2) and bribing a foreign official (section 6). Importantly the offences cover conduct that is business to business as well as business to government official. It also, unlike the FCPA, covers facilitation payments.

The Act also for the first time introduced a new strict liability corporate offence of failure to prevent bribery, where the only defence available is to show that the corporate body has/had "adequate procedures" in place to prevent bribery which are proportionate, involve top level commitment, are the result of periodic risk assessments taking into account jurisdiction, sector, size of the organisation; undertaking of appropriate due diligence on persons performing services and people they deal with; communication to the employees including training and monitoring and review. A company can also be held criminally liable for the substantive offences under section 1, 2 and 6 if the prosecution can prove that the controlling mind of the company was involved in or complicit in the acts. The controlling mind test is a difficult one to meet and is generally understood to mean an individual with express decision making powers who can speak on behalf of the company, usually a director or board member.

The legislation has extra territorial effect in so far as no part of the offence need be committed in the UK, so long as the offender has a close connection to the UK (citizen, body incorporated in the UK). The corporate offence of failing to prevent is not limited to acts in the UK so long as the companies incorporated or formed in the UK or carries on part of a business in the UK.

The maximum sentence for sections 1, 2 and 6 is 10 years for individuals and an unlimited fine for bodies corporate. There is no maximum fine for the corporate offence of failing to prevent bribery. In relation to the prosecution of a corporate, this can be dealt with by way of a deferred prosecution agreement; whey by the corporate avoids a conviction by paying a large fine, disgorging the profits from the bribery and undertaking a monitored remediation plan.

These types of cases are usually prosecuted by the Serious Fraud Office.

Q1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

Craig Weston

(iii) Insider Dealing:

The main piece of legislation in relation to Insider Dealing is section 52 Criminal Justice Act 1993. Insider dealing is where a person who has inside information (generally meaning information not in the public domain) about securities (e.g. shares) does one of the following whilst in possession of the inside information: (i) deals in those securities on a regulated market (this includes spread betting and Contracts for Difference (CFDs)); (ii) encourages someone else to deal in those shares or recommends that someone cancels their order to purchase shares; or (iii) discloses the information to another person, when he wasn't allowed to do so (e.g. in breach of his employment contract).

Insider dealing can be prosecuted under s52 of the Criminal Justice Act 1993; the maximum penalty is seven years imprisonment and/or a fine. It can also be dealt with as a regulatory matter under Article 14 of the Market Abuse Regulation for which the penalties include a fine and/or a ban from working in financial services. The Financial Conduct Authority is the regulator/prosecutor which investigates and prosecutes cases of insider dealing.

Esra Bicen

(i) Corporate Fraud:

Turkish jurisdiction defines corporate fraud to include accounting fraud schemes, falsification of financial information, self-dealing by corporate insiders, obstruction of justice, tampering with witnesses, perjury and other behaviour relating to falsification and self-dealing activities.

The main legislation dealing with corporate fraud is the Turkish Commercial Code, the Tax Procedure Code and the Turkish Penal Code. Commercial Code and Tax Procedure Code include detailed provisions regarding bookkeeping and financial reporting standards, prohibition of self-dealing by shareholders and executives and liability provisions.

Turkish Commercial Code remedy provisions include corporate derivative actions, executive and shareholder liability lawsuits and reimbursement of dividends and proceeds of self-dealing transactions.

Tax Procedure Code liability provisions impose administrative and criminal penalties for fraud schemes resulting in tax evasion and tax loss and fines for irregularities and deviations from statutory form requirements.

(ii) Securities Fraud:

Capital Markets Law is the primary legislation with law enforcement provisions regarding securities fraud. Main statutory definitions of securities fraud include insider trading, market manipulation, accounting fraud and irregularity in financial reporting. Enforcement provisions cover cancellation of transactions, orders, imprisonment of beneficiaries, shareholders, board members and executives and judicial fines imposed upon financial institutions.

(iii) Banking Fraud:

Banking Act is the main legislation governing liability provisions regarding bank fraud. Main banking crime definitions include false statements, out of book transactions, falsifying accounting records, embezzlement, manipulating data and information systems. Banking Act imposes personal liability upon bank majority shareholders and executives for any such criminal activity and misappropriating resources of the banks. Remedial measures include imprisonment and judicial fines, reimbursement of proceeds and indemnification of losses, seizure of shares by the Savings Deposit Insurance Fund ("SDIF").

Q1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

Esra Bicen

(iv) Bankruptcy Fraud:

Execution and Bankruptcy Code defines bankruptcy fraud schemes as engaging in fraudulent transactions with the intent to defraud creditors before or after filing for bankruptcy. Liability attaches to corporate executives and beneficiaries acting with intent. Penalty provisions include imprisonment and judicial fines.

(v) Bribery and Corruption:

Tax Penal Code includes provisions regarding bribery, corruption forgery, counterfeiting, procurement fraud, perjury, obstruction of justice, tampering with evidence, embezzlement, and penalty and law enforcement provisions such as judicial fines and imprisonment, seizures and confiscation of goods and revenue, cancellation of operation licenses.

Jodi Avergun

(i) Corporate Fraud:

Unlike many other countries, a corporation can be charged with committing crimes in the United States. The wire and mail fraud statutes are the primary vehicles through which U.S. prosecutors charge companies.

Mail and Wire Fraud: 18 U.S.C. §§ 1341 and 1343

Mail and Wire Fraud Elements:

- Defendant engaged in a scheme to defraud;
- Defendant acted with the specific intent to defraud;
- The scheme resulted, or would result upon completion, in the loss of money, property, or honest services; and
- The U.S. mail, a private courier, or interstate or international wires were used in furtherance of the scheme to defraud, and
- Defendant used, or caused the use of, the mail, courier, or wires.

The federal wire fraud statute also includes offenses involving computers and the internet.

(ii) Bribery and Corruption:

The Foreign Corrupt Practices Act: 15 U.S.C. §§ 78dd-1, et seq.

The Foreign Corrupt Practices Act ("FCPA") prohibits making payments to foreign government officials to assist in obtaining or retaining business.

FCPA Elements:

- Use of the mails or any means of instrumentality of interstate commerce;
- By a covered person;
- An offer, payment, promise to pay, or authorization of the payment of money or anything of value;
- To a foreign official to influence the foreign official in his or her official capacity;
- To secure any improper advantage in order to obtain or retain business.

"Covered person" includes issuers of registered securities in the U.S., domestic concerns, officers, directors, employees and agents of domestic concerns or issuers, and foreign individuals and companies who commit acts in furtherance of corrupt payments while in the U.S. or who cause others to do so.

Q1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

Jodi Avergun

(iii) Insider Trading:

Section 10(b) of the Securities Exchange Act of 1934: 15 U.S.C. §§ 78j

Insider trading in securities may occur when a person in possession of material non-public information about a company then buys or sells that company's stock to make a profit or avoid a loss. The law prohibits the use of manipulative or deceptive means in the purchase or sale of securities. Its implementing regulation is Rule 10b-5.

The elements of an insider trading charge are:

- Defendant engaged in "manipulative or deceptive" practices
- in connection with the purchase or sale of a security,
- in violation of SEC rules; and
- Defendant acted wilfully.

Rule 10b-5 requires proof that a defendant:

- engaged in a fraudulent scheme,
- made a material misstatement, or
- omitted material information to a person whom the Defendant owed a duty;
- The scheme, misstatement, or omission occurred in connection with the purchase or sale of a security; and
- Defendant acted wilfully.

Q2. What international conventions apply in your jurisdiction?

Dennis Miralis

Australia is a signatory to a number of international conventions which impact on the area of economic crime. The key global conventions include the United Nations Convention Against Corruption, an international treaty that bans corruption and obliges signatory states to take a large variety of measures to fight it; the OECD Anti Bribery Convention, which is the first and only international anti-corruption instrument focused on the 'supply side' of the bribery transaction; and the UN Convention against Transnational Organised Crime which requires signatory countries to take measures to prevent and criminalise corruption and curb money laundering and provides a broad network in reinforcing co-operation on these matters. Finally Australia is a signatory to the Budapest Convention on Cybercrime which is becoming more prevalent in Australia. This convention is especially important in the area of mutual assistance and international co-operation as cybercrime based fraud continues to exponentially increase in Australia. Notwithstanding these international conventions, enforcement remains the key determinant of success and by this criteria there is room for improvement.

Angela Barkhouse

As a UK Caribbean overseas territory, the Cayman Islands cannot sign or ratify international conventions in its own right. Rather, the UK is responsible for the Cayman Islands' international affairs and may arrange for the ratification of any convention to be extended to the Cayman Islands which include:

- The United Nations Convention against Transnational Organised Crime
- The United Nations Convention against Corruption; and
- The Organisation for Economic Co-operation and Development Anti-Bribery Convention

Q2. What international conventions apply in your jurisdiction?

Esra Bicen

International conventions applicable in Turkey are:

- United Nations Convention Against Transnational Organised Crime (Palermo Convention)
- United Nations Convention Against Corruption
- United Nations Global Action Plan Against Organised Transnational Crime
- United Nations Global Program Against Money Laundering
- OECD Convention on Combating Bribery of Foreign Officials in International Business Transactions
- European Convention on Mutual Assistance in Criminal Matters
- Treaty on Extradition and Mutual Assistance in Criminal Matters between the United States of America and The Republic of Turkey

Q3. Can you outline the key fraud and white collar crime trends?

Tobias Eggers

(i) In terms of offences:

In 2018, the parliament implemented the new Data Privacy Act which will undoubtedly lead to countless investigations. Companies who have in the past not been acute with the data of their employees and customers will face severe problems. Also quite new: there have been some changes on the money laundering front. Not only will companies now have to really evaluate their money laundering risks (note: you will face damages even if innocent, come an investigation) but to reconsider their compliance management system and adapt to the new regime. Plus, the Financial Intelligence Unit grew and professionalised in 2018 and are now ready to roll. We already see the impact they are having. Also in 2018, new capital market rules have been introduced (more complex than before) and we will see landmark decisions flowing from Dieselgate (part of which is a market manipulation investigation).

(ii) In terms of procedural issues:

Most importantly, if an international law firm will conduct an internal investigation, the law firm can be searched and their findings seized as they cannot fully rely on German constitutional rights. Also, other law firms will have to find ways to protect their products of an internal investigation. Sovereignty over your information is key in an investigation. The state will always be stronger. But if you have sole reign over your information you will be better able to negotiate.

(iii) Buzzing:

In the near future Germany will finally introduce a criminal liability for companies. So far law makers and experts have not seen reason for that (as there are other measures that would have the same effect). But politicians nowadays are determined and as late as 2018 introduced a draft that not only includes provisions for criminal liability of companies but also defendants' rights (right to silence, right to see the prosecutors files, etc.).

" Sovereignty over your information is key in an investigation. The state will always be stronger. But if you have sole reign over your information you will be better able to negotiate."
- Tobias Eggers -

Q3. Can you outline the key fraud and white collar crime trends?

Dennis Miralis

There has been a steady increase in cybercrime actors targeting Australia for profit. These are predominantly groups based offshore, and their activities can be difficult to disrupt due to their highly technical nature, and the use of various anonymising techniques. More specifically, the following types of financially-motivated cybercrimes are increasingly posing a risk to the Australian public, the government, and businesses, including:

- credential-harvesting malware: used to extract account and password information such as banking login details for financial gain;
- ransomware: blocking an individual's access to their computer or files and requesting a 'ransom' to be paid;
- distributed denial of service extortion: threatening to disrupt a business by preventing legitimate access to online services (typically a website) unless a fee is paid;
- Business Email Compromise: targeting businesses for financial gain by impersonating a high-level executive to elicit payment;
- Other areas of increased concern identified by the regulators include the following kind of investment and financial market fraud;
- Fraudulent investment schemes, such as Ponzi schemes, where victims are lured in with the promise of high financial returns;
- Manipulation of the share market to artificially raise or lower the price of shares for financial gain;
- Exploitation of financial securities for financial gain or to launder the proceeds of crime.

Angela Barkhouse

The Cayman Islands is home to a well-developed financial centre that provides a wide range of services, including banking, structured finance, investment funds, various types of trusts, and company formation and management. As such in a risk assessment strategy undertaken by the Cayman Islands government, the more common types of white collar crime identified are related to theft, corruption and the evasion of tax by overseas residents.

There has also been attention on the potential risks in crypto currency and the likelihood of fraud. A recent Wall Street Journal article cited that from a review of 1,450 initial coin offerings ("ICO's"), an alarming 20% had 'red flags, including plagiarised investor documents, promises of guaranteed returns and executive teams that go missing after funds have been raised. The SEC has increased its focus on ICO's bringing its first enforcement action in late 2018. The interest in ICO's continues unabated as does the reporting in suspected fraud demonstrating the need for ICO's to become properly regulated to ensure the legitimacy of these projects.

Esra Bicen

(i) Banking Fraud:
Key banking fraud trends include misappropriation of bank resources, false representation and obstruction of justice (i.e. failing to provide information and documents requested by official authorities).

(ii) Securities Fraud:
The main categories of securities fraud cases include insider trading, market manipulation and market abuse.

(iii) White-Collar Crime:
The main categories of white-collar crime typologies include self-dealing of corporate executives, corruption, money laundering, unauthorised financial operation (exchange offices), perjury, falsifying accounting records and financial statements, suspicious cash movement and tax evasion.

Q3. Can you outline the key fraud and white collar crime trends?

Jodi Avergun

In 2019, prosecutors in the U.S. are likely to continue to focus on large multi-national cases involving fraud in the anti-corruption space. The DOJ's new "no piling on" policy virtually assures increased cross-border cooperation with corporates more likely to be prosecuted in the jurisdictions in which misconduct occurred and with penalties appropriately apportioned among interested countries.

The term "piling on" comes from American football — the practice where a player jumps on a pile of other players who have already sufficiently tackled the opposing player. It's a dangerous practice in sports or law enforcement, and global companies have paid the price. Accordingly, to encourage coordination among DOJ components and other enforcement agencies when imposing multiple penalties for the same conduct the anti-piling on policy was announced.

The "aim" of the new policy "is to enhance relationships with our law enforcement partners in the United States and abroad, while avoiding unfair duplicative penalties." In the Justice Department's view, piling on may "deprive a company of the benefits of certainty and finality ordinarily available through a full and final settlement." DOJ prosecutors are instructed to consider the egregiousness of a company's misconduct; statutory mandates regarding penalties, fines, and/or forfeitures; the risk of unwarranted delay in achieving a final resolution; and the adequacy and timeliness of a company's disclosures and its cooperation with the Department in "determining whether coordination and apportionment between Department components, and with other enforcement authorities, allows the interests of justice to be fully vindicated."

Another likely trend is an increase in declinations under the DOJ's FCPA Corporate Enforcement Policy. In a series of speeches during 2018, the Department of Justice outlined its enforcement policies in an effort to define precisely the outcome of for a company of voluntary self-disclosure of corporate fraud or other misconduct in. According to DOJ officials, if a company voluntarily discloses misconduct, fully cooperates with the DOJ and performs timely and appropriate remediation, including disgorgement of ill-gotten gains, making restitution and agreeing to forfeit-tainted assets, he added that the DOJ's FCPA Corporate Enforcement Policy "also enumerates a non-exhaustive list of aggravating circumstances that can overcome that presumption." Even where a declination is not possible, companies can still obtain reduced fines and penalties as long as there is remediation and full cooperation.

Q4. Have there been any recent regulatory changes or interesting developments?

Dennis Miralis

The Australian Government established a Royal Commission into the alleged misconduct of Australia's banks and other financial services entities in 2017. In 2018, the Inquiry considered the conduct of banks, insurers, financial services providers and superannuation funds (not including self-managed superannuation funds). Over the course of 68 days, the inquiry heard evidence from 134 witnesses.

The Royal Commission specifically focused on how well equipped regulators are to identify and address misconduct. This has been one of the most significant developments in the area of white collar related activity for some time. The interim report which was released in September 2018 highlighted deficiencies in Australia's treatment of financial institutional misconduct. The final report is due to be tabled in February 2019. It is anticipated that as a result of the findings of the Royal Commission that there will be a significant increase in funding to the Commonwealth Prosecutors to investigate and prosecute white collar offending by financial institutions and individuals in the finance sector. An attitudinal change towards white collar crime is clearly underway in Australia and this will lead to more aggressive regulation and enforcement, similar to what we see in other Western jurisdictions.

Q4. Have there been any recent regulatory changes or interesting developments?

Dennis Miralis

Another area where the Australian Government has been particularly focused concerns amending the powers of the corporate regulator (ASIC) and the laws it administers. Presently the Australian Government is looking to pass new laws where the biggest changes will be the increase in the term of imprisonment for criminal offences as well as larger financial penalties imposed for both criminal offences and civil contraventions under the Corporations Act 2001, Australian Securities and Investments Commission Act 2001 (ASIC Act), National Consumer Credit Protection Act 2009 and Insurance Contracts Act 1984. Additional changes being looked at include the courts may now give priority to compensating victims over the payment of financial penalties:

- introduction of a new "ordinary standards" test that applies to all dishonesty offences under the Corporations Act;
- introduction of relinquishment of any financial benefit gained from conduct that contravenes civil penalty proceedings;
- extending the infringement notice regime;
- and courts will also be empowered to consider even greater penalties where the profits from misconduct are high or where a company's annual turnover exceeds $105 million.

Angela Barkhouse

Most recently, the Cayman Islands International Tax Co-operation ("Economic Substance") Law, 2018 ("The Law") came into force on 1 January 2019. The Law requires "in-scope" entities that carry on particular activities to have demonstrable economic substance in Cayman. The Law defines which Cayman entities are in-scope ("Relevant Entities"). Relevant Entities must make an annual report as to whether or not they are carrying on one or more of a defined list of activities ("Relevant Activities").

Under the Regulations, a relevant entity that is carrying on a relevant activity and is required to satisfy the economic substance test shall prepare and submit a report ('Report') to the Tax Information Authority ('TIA') no later than 12 months after the last day of the end of each financial year of the relevant entity commencing on or after 1 January 2019.

The enactment of the Law is designed to meet the Cayman Islands 2017 commitment as an Inclusive Framework member under the OECD's global Base Erosion and Profit Shifting initiative.

In addition, the Cayman Islands beneficial ownership regime ("the Regime") came into force on 1 July 2017. The Regime requires Cayman Islands companies and limited liability companies ("LLC's") to establish and maintain a register of beneficial ownership, (unless they fall within an available exemption under the Regime). Filings must have been made on or before 29 June 2018 to avoid liability for offences under the Regime.

The records filed must declare details of the individuals who ultimately own or control more than 25% of the equity interests, voting rights or have rights to appoint or remove a majority of the company directors, or LLC managers, together with details of certain intermediate holding companies through which such interests are held.

The requirement is pursuant to a commitment agreed with the UK Government (by way of an Exchange of Notes in April 2016) by the Cayman Islands and other Crown dependencies and overseas territories. Its objective is to enhance existing arrangements on the exchange of beneficial ownership information, thus further assisting law enforcement agencies in the combatting of tax evasion and money laundering.

Q4. Have there been any recent regulatory changes or interesting developments?

Craig Weston

2017/2018 saw a number of new investigative tools and criminal offences introduced into the world of white collar crime in the UK with two aims: (i) to make it easier to seize criminal assets and (ii) to make it easier to hold corporates criminally liable.

Most notably and with greatest public and media fanfare was the introduction of Unexplained Wealth Orders in the Criminal Finances Act 2017. Primarily an investigative tool, they are a High Court order requiring the recipient to explain the source of his/her wealth where there is an apparent disconnect between the known sources of income/ wealth and for example the value of an assist that is owned. This is aimed at serious organised crime and corrupted PEPS. If the recipient cannot sufficiently explain the source of the legitimate wealth for a particular asset such as a house then the court automatically deems that house to be criminal property and can take steps to seize it.

The same piece of legislation introduced Account Freezing and Forfeiture Orders. These tools allow a variety of law enforcement agencies to freeze bank accounts they suspect of holding the proceeds of unlawful conduct or money which could be used in unlawful conduct. Previously law enforcement agencies did not have the power to freeze or forfeit money in such accounts. After the money has been frozen they can apply, once an investigations has been completed, to have the contents of the bank account forfeited. The test applied by the courts is on the balance of probabilities and applications for ARFO's are heard in the Magistrates Court.

The final gift of the Criminal Finances Act 2017 was to introduce two new offences relating to corporates: (i) failing to prevent the facilitation of tax UK tax evasion and (ii) the failure to prevent the facilitation of foreign tax evasion. This is similar in model tot the UK Bribery Act and is strict liability but affords a defence where the company has put "reasonable prevention procedures" in place. It is aimed at the professional services sector such as lawyers, accountants and financial advisers and aims to criminalise advice and assistance in how to evade tax given to those liable to tax. For example, it would cover an accountancy firm where one of their accountants dishonestly assist a client tax payer to under declare tax, or a company that routinely engages in not applying VAT where it should. It is too early to tell if this will be a widely used offence and if it will have the desired impact but it is a window in the UK Government's mind and indicates the direction of travel in relation to corporate criminal liability.

Jodi Avergun

In the context of securities fraud, one of the most interesting developments was the decision of the U.S. Supreme Court in *Lucia v. United States*, a case involving the constitutionality of administrative law judges ("ALJ"s). The case arose as a result of the increased number of cases SEC attorneys chose to bring in their "in house" administrative court as opposed to in Federal District Court where there is a more level playing field. The question in Lucia was whether administrative law judges of the SEC were properly appointed under the U.S. Constitution. Prior to Lucia, SEC ALJs were selected without any presidential or Commission appointment, calling into question the authority of their position.

On 21 June 2018, the Supreme Court ruled that SEC ALJs were officers of the United States within the meaning of the appointments clause. The Court found that SEC ALJs exercise "significant discretion" while carrying out "important functions." Justice Kagan wrote that the SEC's ALJs possess significant discretion as they have "nearly all the tools of federal trial judges" to ensure fair and orderly adversarial hearings. They also serve on an on-going basis and are given career appointments. The Court ordered a new proceeding for the petitioner, Raymond Lucia, with a properly appointed ALJ and specified that the new ALJ cannot be the one who originally heard the case.

In the wake of the Lucia decision, the SEC granted all respondents in the proceedings previously on hold the "opportunity for a new hearing before an ALJ who did not previously participate in the matter," and remanded all pending cases before the Commission to the Office of the ALJs "for this purpose." Additionally, the order vacated "any prior opinion"

Q4. Have there been any recent regulatory changes or interesting developments?

Jodi Avergun

issued by the Commission in over 125 pending matters, so those which had not exhausted their appeal rights could be afforded a new hearing with a different ALJ.

While the appointments issue has now been addressed for future administrative proceedings, there are still questions surrounding the SEC's use of administrative proceedings ("APs"). It will be interesting to see if the SEC returns to an aggressive use of administrative proceedings in all kinds of cases, or whether it will take a more limited approach. There are also other challenges to the SEC's administrative proceeding process that remain unresolved, including claims that ALJs are improperly insulated from discipline and cannot be removed for misconduct. While plaintiffs have not had much success based on these arguments, it is likely they will continue to push them going forward.

Q5. How is the continuous development of smart technology impacting fraud and white collar crime?

Tobias Eggers

We see changes within compliance management systems of companies. By investing in technology-driven data analytics solution companies are now trying to minimise the occurrence of fraud. According to the ACFE, organisations that lacked anti-fraud controls suffered twice as much in median losses compared to organisations with proactive data monitoring/analysis systems and fraud hotlines. So, big international companies have understood that they will have to take money in their hands. However, that is not true for smaller companies that still see compliance rather as a nuisance.

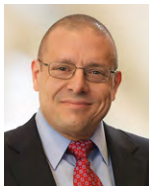
Law firms such as ours, who conduct internal investigations, have long been using all sorts of smart tech in order to analyse data and find criminal conduct. The same goes for public prosecutors. They however are mostly relying on police who usually take their time. Here lies a key advantage we as lawyers have over prosecution. We can act faster as we do not have to rely on other institutions to react.

Dennis Miralis

The use of cryptocurrencies in the area of organised fraud and money laundering has been noted globally. In Australia there have now been a number of criminal prosecutions where bitcoin has been identified as being the means by which proceeds of crime have been laundered. Additionally, the Crime Commissions have successfully frozen bitcoin accounts and it has been forfeited to the Australian Government as proceeds of crime. The use of the internet to foster sophisticated cyber frauds has also continued to increase with enforcement activity against offshore organised groups being very difficult to pursue. In this regard the Australian Government has allowed increased capabilities to be provided to Australian law enforcement to adopt a proactive and offensive approach to targeting cybercrime including using the capabilities of the military. The success of this approach is too early to assess as these are new capabilities. Notably, Australia became the first country in the world to introduce legislation in December 2018, which is aimed at curbing the use of encryption technology to mask serious criminal activity. This was in response to the perceived increase use of anonymising technology to frustrate criminal investigations. The use of such legislation compelling technology companies to assist law enforcement undermines encryption which is highly controversial.

"The use of the internet to foster sophisticated cyber frauds has also continued to increase with enforcement activity against offshore organised groups being very difficult to pursue.@
- Dennis Miralis -

Q5. How is the continuous development of smart technology impacting fraud and white collar crime?



Salvatore LaScala

While there have certainly been improvements in technology in recent years that have advanced financial crime detection, the industry has, in some ways, lagged. For example, detecting fraud, which includes a return on investment, is fairly advanced while anti-money laundering, which does not indicate a "return on investment" or enhance the bottom line, has long been deploying rules-based systems to conduct transaction surveillance for the detection of potentially suspicious activity. These rules-based systems require constant testing and optimisation — yet a high rate of false positives is typical throughout the industry. Moreover, advancement has slowed with respect to detecting new money laundering typologies.

Artificial intelligence (AI), specifically machine learning, is the first innovation in years with the promise to significantly enhance our ability to detect and prevent financial crimes of all categories, especially money laundering. To be clear, AI technology is not new. For the past decade, data scientists have worked to make machine learning accessible and adaptable. The complex algorithms have been written, the keys to manipulating massive data sets are known, and the technology is universal enough to be applied to different problems. Now it is up to financial institutions to make the leap and use AI and machine learning to detect human traffickers, narcotics and arms sales, terrorist payments, and the money laundering that fuels these activities.

AI technology will completely change the way we go about rooting out this activity. Using unsupervised learning (the process by which a model draws inferences from uncategorised data to analyse and identify patterns and underlying structures), transaction-monitoring models can group customers according to their behaviour and then flag truly anomalous behaviour that is potentially suspicious. This is unlike a rules-based system, where customers may be segmented by basic characteristics. Anomaly detection is not as effective because (i) the customers are not grouped by behaviour, and (ii) someone has to write the rules to catch every potential anomalous behaviour, of which there is a limitless supply. Machine learning is allowing banks to home in on truly anomalous behaviour that is potentially suspicious. And this is leading us to discover new financial crime red flags in real time — rather than waiting for law enforcement and regulators to report them to banks.

Angela Barkhouse

As technology develops so does the variety of cyber crimes. In recent years, we have seen offences such as ransomware – a type of online attack that blocks victims' access to their computers until they pay a ransom –become more prevalent.

In turn, however, the development of smart technology itself now forms a substantial part of any investigation and indeed in evidence. It is no longer sufficient to be able to understand financial investigations, analysis, and accounting; investigation firms now need to know how to access and secure data from mobile devices, social media, Fitbits and other devices that store computerised data, and the so-called "dark web", to ensure any expert reports are admissible in a court of law.

Moreover, as the amount of data increases, investigators are using powerful databases, to review unstructured or "big" data and online or digital information text with advanced analytic tools to identify and expose financial crimes. New technology is making it easier to follow the money trail, both in terms of time, cost and resource, accelerating the analysis. It is also able to graphically visualise financial transactions and flow of funds patterns that are much more user friendly than scores of excel spreadsheets. Indeed, the most effective litigator in the courtroom is the one who uses forensic technology and investigative support, to provide clarity to the court in support of their arguments.

Finally, the new development of automated translation tools to assist in the analysis of multi-language documents of significant size in cross border investigations and litigation is becoming increasingly needed, and I suspect these will advance significantly in the next few years.

Q6. Have there been any noteworthy case studies or examples of new case law precedent?

Esra Bicen

Following the 2015 attempted military coup, SDIF took over management of numerous private companies found to be associated with the FETÖ terrorist organisation ('Cleric Gulen movement') or involved in terrorist financing under Turkish Criminal Procedure Code articles 128 and 133. Based on the information provided by SDIF on its website, as of 5 March 2018, the total number of companies, managements of which are taken over by SDIF, is 1124. Most of these seizures are related to the FETÖ prosecutions. Although SDIF has very broad law enforcement powers under the Banking Act article 107, including transferring shares of seized banks to third parties, Turkish Criminal Procedure Code articles 128 and 133 do not allow for taking over the ownership of the shares but only allows for temporary takeover of the management of a company engaged in criminal activity. This raises a new debate that SDIF could face a wave of highly debatable lawsuits before international arbitration forums initiated by international investors holding shares in these companies involving restitution of shares claims.

Angela Barkhouse

In the landmark case of *Ahmad Hamad Algosaibi & Brothers (AHAB) v Saad Investment Finance Corporation Ltd and Others*, 2018, AHAB brought proceedings against Maan Al Sanea who had married into the Algosaibi family, and who had become the Managing Director of a family owned business the Money Exchange in 1981, and established his own 'Saad Group' through various vehicles including a number of Cayman Islands companies and trusts. The proceedings turned into a decade long investigation and a trial that lasted over a year in the Grand Court of the Cayman Islands.

In 2009, the global financial crisis impacted AHAB's credit lines and AHAB defaulted on billions of Saudi Riyals of debt. Shortly after that default, AHAB commenced the proceeding against Al Sanea and 42 corporate defendants (who were part of, or did business with, the Saad Group) to recover US$9.2bn, being the amount of borrowing that was not repaid at the time of the default and representing the proceeds of a fraud AHAB alleged had been perpetrated against AHAB by Al Sanea.

AHAB sought to argue that previous case law in (a) *Relfo Limited (in liquidation) v Varsani* [2014] and *Federal Republic of Brazil and another v Durant International Corp* [2015] established that the Court could infer that funds were the traceable property of AHAB and (b) AHAB could elect to follow its beneficial interest into the hands of the Defendants who were then required to give an account of how they acquired it. The claimants argued that the Defendants had failed to give a proper account and AHAB could thus locate its beneficial interest in the property presently held by each Defendant.

AHAB's claims were primarily proprietary in nature seeking to recover what AHAB said was its property from the Defendants. The proprietary claims were essential to AHAB's success because, unless AHAB proved that the assets held by the Defendants were its property, AHAB would be unable to secure priority over the existing contractual claims of third party banks, which had been admitted as debts in the respective liquidations of the Defendants.

The Grand Court however rejected these arguments. Instead it held that whilst the law may infer the necessary transactional links to give rise to a tracing claim where there is a scheme "specifically designed" to subvert the ability of creditors to recover misappropriated funds, the general rule remains that it is necessary to establish a chain of transactions in order to trace funds. Moreover, whilst a defaulting trustee or fiduciary is required to account for what has become of the trust funds under their hands that did not absolve AHAB of the burden of demonstrating that particular funds were trust assets.

Put simply, in the case of theft or embezzlement of funds, the ability to infer beneficial ownership of a defendant's assets is not sufficient even if breach of trust exists, an arguable case will still require the claimant to provide a detailed tracing exercise of the financial transactions to the Defendant, believed to have been in unlawful receipt of these funds.

Q6. Have there been any noteworthy case studies or examples of new case law precedent?

Craig Weston

Recent years have been unprecedented in the UK for noteworthy cases in the sphere of white collar crime, in particular cases investigated and prosecuted by the Serious Fraud Office and the increased use of DPAs.

2017/2018 saw the SFO enter into Deferred Prosecution Agreements with two of the UK's largest multinational companies. The DPA with Rolls Royce was approved by Sir Brian Leveson, President of the Queen's Bench Division on 17 January 2017. The DPA enables Rolls-Royce to account to a UK court for criminal conduct (primarily bribery and corruption) spanning three decades in seven jurisdictions and involving three business sectors.

The DPA involved payments of £497,252,645 (comprising disgorgement of profits of £258,170,000 and a financial penalty of £239,082,645) plus interest. Rolls-Royce are also reimbursing the SFO's costs in full (c£13m). This represents the largest ever fine levied on a UK company. The investigation into the conduct of individuals continues but the DPA above is based on an acceptance by Rolls Royce that the SFO had evidence of bribery and corruption sufficient to meet the controlling mind test.

In April 2017, the SFO announced that it had entered into a DPA with Tesco Stores Limited subject to compliance with the terms of the DPA, the investigation by the SFO into Tesco plc and Tesco Stores Ltd is concluded. The DPA only relates to the potential criminal liability of Tesco Stores Limited and does not address whether liability of any sort attaches to Tesco plc or any employee, agent, former employee or former agent of Tesco plc or Tesco Stores Ltd. Tesco plc took a total exceptional charge of £235m in respect of the DPA of £129m, the expected costs of an FCA compensation scheme of £85m, and related costs. This has been recorded in the financial statements in the year to 25 February 2017 of Tesco plc as an adjusting post balance sheet event. The DPA had not been released in full due to the reporting restrictions pending the conclusion of the trial of the senior executives. Three former Tesco employees who held senior management roles in the Tesco UK business were charged over allegations of fraud. The alleged activity occurred between February and September 2014. In a retrial of Christopher Bush and John Scouler, which began on 1 October 2018, His Honour Sir John Royce handed down a no case to answer judgment on 26 November 2018. The Court of Appeal on 5 December upheld the decision by the Judge that there was insufficient evidence for a jury to consider in respect of the individual defendants on trial and ordered an acquittal. There is an outstanding executive.

The recent and upcoming trials of the individuals alleged to be the basis for the conduct accepted in DPA's has thrown up some interesting issues relating to the admissibility of the DPA in their trials, the investigation process undertaken by the SFO in conjunction with the companies the subject of the DPA and whether individuals right to a fair trial can be properly protected under the DPA regime.

This has led to two significant pieces of litigation on the issue of privilege in internal investigation prior to a self-report to the SFO. In ENRC the matter bounced backwards and forward, at first instance a ruling by Mrs Justice Andrews's narrowly applied the Three Rivers judgement leading to a position where notes taken in internal investigation interviews would to be privilege as they were not in contemplation of litigation. This was to a certain extent reversed in the Court of Appeal accepting that although a fact specific matter there could be reasonable contemplation of proceedings without having been charged or prior to a self-report.

"Recent years have been unprecedented in the UK for noteworthy cases in the sphere of white collar crime, in particular cases investigated and prosecuted by the Serious Fraud Office and the increased use of DPAs."
- Craig Weston -

Q6. Have there been any noteworthy case studies or examples of new case law precedent?

Craig Weston

The second case in *AL v SFO* [2018] EWHC 856 Agreement concerned the extent to which the Serious Fraud Office, in fulfilling its disclosure obligations towards a defendant in criminal proceedings, is under a duty to obtain documents from a company with which it had concluded a DPA, where that company was required to afford total cooperation to the SFO under the DPA but had refused to provide the documents, asserting legal privilege. The Claimant sought judicial review of the SFO's decision not to pursue the company for breach of the duty of cooperation under the DPA for its refusal to hand over the documents. The Divisional Court (Holroyde LJ and Green J) held that the High Court was not the appropriate forum in which to resolve this kind of dispute about disclosure, but also expressed serious reservations about the SFO's position, holding that – if the High Court had been the proper forum – it would have quashed the SFO's decision.

Finally in our bumper 2018, the High Court has considered an issued that has been vexing lawyers for years. The High Court has held in *KBR Inc v The Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin) that the SFO can lawfully require companies and individuals to produce material held abroad, subject to there being a sufficient connection with the UK, through its use of its Section 2 Notice powers (compelled information requests).

Jodi Avergun

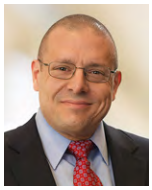
The U.S. Court of Appeals for the Second Circuit handed the Department of Justice a rare defeat on 24 August 2018 by holding that prosecutors could not assert conspiracy or aiding and abetting liability to effectively circumvent the jurisdictional language of the Foreign Corrupt Practices Act.

In *United States v. Hoskins* (902 F.3d 69 (2d Cir. 2018)), the Second Circuit grappled with whether a foreign national who could not be charged as a principal for violating the FCPA could be guilty as a co-conspirator or an accomplice. In reviewing the language of the FCPA as well as its legislative history, the Second Circuit affirmed the decision of the district court and found that the DOJ's overly broad jurisdictional argument was beyond what the U.S. Congress intended for the statute.

While the Second Circuit nonetheless permitted the case to proceed on an agency theory of liability, the ruling may prompt defendants that are not clearly subject to the FCPA, such as unaffiliated third parties operating outside the United States, to push back against aggressive prosecutions that for decades have largely gone unlitigated and therefore unchecked by the courts.

The initial beneficiaries of the Hoskins decision are likely to be foreign-based joint venture partners of, or consultants to, U.S. companies or their foreign subsidiaries who act solely outside the United States. However, its longer-term impact on how the DOJ prosecutes foreign bribery offences against individual and corporate defendants remains to be seen. One possibility is that the DOJ will be forced to spend more effort establishing the basis for an agency relationship for non-U.S. defendants – an issue that may already have been impacted by developments in the Hoskins case. Another possibility is that, rather than engaging in legal contortions to allege an agency relationship, the DOJ will use money laundering and other statutes that can adequately address bribery charges. The federal money laundering statute has extraterritorial application and does not exempt any particular class of defendant from punishment. In addition, the FCPA is an offence that is specifically enumerated in the money laundering statute, as if the financial transaction at issue is intended to promote or conceal, it would violate the law. The Hoskins decision may also accelerate the trend, as seen in *Rolls-Royce, United States v. VimpelCom Ltd*, and *United States v. Keppel Offshore & Marine Ltd*, of the DOJ partnering with and assisting foreign law enforcement agencies to pursue their own bribery prosecutions against non-U.S. nationals acting outside the United States. Each case generated significant financial settlements for the foreign regulators – which are certainly an incentive to aggressively pursue such a strategy going forward.

Q7. What is the difference between unlawful and unethical conduct and to what extent has the line become increasingly blurred in recent years?



Salvatore LaScala

Unlawful conduct is behaviour that is expressly prohibited by a specific legal constraint (i.e., statute, regulation) that can trigger sanctions or penalties (i.e., monetary fines, imprisonment). Unethical conduct on the other hand is behaviour that, while not technically illegal, is generally considered immoral.

Just because conduct may be legal doesn't mean it's ethical. For example, some executives would argue that their primary responsibility is to the organisation's shareholders and that as long as their actions to maximise profits are legal, it's irrelevant that their behaviour may be considered unethical. Others argue that companies have a responsibility to society as a whole to not only behave legally, but also (and perhaps more importantly) behave ethically.

As the line between illegal and unethical behaviour blurs and the focus on the social responsibility of corporate leadership increases, corporations have increasingly focused their compliance programs on both illegal and unethical conduct.

Craig Weston

Traditionally in the UK, the line between unlawful conduct and unethical conduct has been drawn as conduct between which the Government has legislated to make it illegal/unlawful and where societal norms or a code of conduct make not reaching the particular standard of conduct or breaching the code of conduct, unethical.

The starkest example in the UK is in relation to the concepts of tax evasion and tax avoidance. Evasion is the unlawful non-payment or non-accounting for tax that is lawfully owed or due. Whereas tax avoidance (which is lawful but in many circles seen as morally reprehensible or unethical) is the practice of using loopholes and schemes designed to lawfully exploit the tax regime to reduce one's tax liability. The public often conflate the two and very public figures in the UK have been vilified when it has been exposed – for example by the Panama Papers – that they were engaging in tax avoidance, despite it not being illegal.

Often the distinction is most readily noticeable in the regulatory context where societal expectation and pressure necessitates a code of conduct and a professional body to enforce that code of conduct. For example, with the work of the Financial Conduct Authority. The FCA regulates the UK financial sector and is both a prosecutor and a regulator. On the one hand it regulates finance professionals by reference to a handbook, rule and a code of conduct, breaches of which can result in regulatory enforcement action such as fines, suspension, restrictions on practice or warnings. On the other hand it can also prosecute criminally for matters such as insider dealing, whereas it can deal with market abuse (based on similar conduct to insider dealing) by way of civil and regulatory powers. Another example may be pension misspelling which is not per se illegal but the FCA has decided that it is unethical and uses its regulatory powers to enforce against those engaging in such behaviour.

Q8. At what point does liability shift between employee and employer? And what measures should businesses incorporate to counteract the increasing regulatory compliance burden?

Craig Weston

In the criminal context this is a question that is currently being considered for review/overhaul by the UK legislature and is the subject of a UK Government call for evidence. This review arises out of a generally accepted view that it is difficult to hold employers/corporates criminally liable for the acts of their employees in the UK by reason of what we call "the identification principle" or "controlling mind test".

As the law currently stands, unless there are specific provisions relating to corporates (such as the failing to prevent bribery offence), for an employer to be held criminally liable it must be proved that an individual in the company, who represents the controlling mind of the company, has committed/is complicit in the offence. This is where 'the acts and state of mind' of those who represent the directing mind and will be imputed to the company, *Lennards Carrying Co Ltd v Asiatic Petroleum Co Ltd* [1915] AC 705, *Bolton Engineering Co v Graham* [1957] 1 QB 159 (per Denning LJ) and *R v Andrews Weatherfoil* [1990] 56 C App R 31 CA. The leading case of *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153 restricts the application of this principle to the actions of the Board of Directors, the Managing Director and perhaps other superior officers who carry out functions of management and speak and act as the company. This identification principle acknowledges the existence of corporate officers who are the embodiment of the company when acting in its business. Their acts and states of mind are deemed to be those of the company and they are deemed to be 'controlling officers' of the company. Criminal acts by such officers will not only be offences for which they can be prosecuted as individuals, but also offences for which the company can be prosecuted because of their status within the company.

One of the issues that the Government consultation is considering is whether the identification principle acts disproportionately on smaller companies and makes it harder for prosecutors to successfully prosecute larger, multinational companies for the acts of their employees. This is because in a smaller company the owners/directors are usually involved in the majority if not all decision making, making it more likely that any criminal acts were undertaken by someone with the controlling mind. The options being looked at by the UK Government include the vicarious liability principles used in the United States, and an extension of the failing to prevent model of offences found in the UK Bribery Act.

In the regulatory context, particularly the regime implemented under the Financial and Services Markets Act 2000, the FCA regularly investigates companies and holds then liable, with civil penalties for the acts of their employees. Again however this is not by using the vicarious liability model, rather a failing to prevent type of approach.

Jodi Avergun

Corporations can be charged with committing crimes. Federal criminal statutes apply to any "person" who violates their prohibitions, including individuals as well as corporations, companies, associations, firms, and partnerships. As a legal entity that exists only in documents, a corporation is incapable of independently forming the mens rea necessary to commit a criminal act. Instead, the corporation acts through its employees and agents.

The most prominent theory of corporate criminal liability is respondeat superior. Originally developed in tort law, respondeat superior holds corporations both civilly and criminally liable for the acts of their employees and agents, so long as the acts were carried out within the scope of their authority and, at least in part, for the benefit of the corporation.

Under respondeat superior, two elements must be present for a corporation to be liable for the criminal acts of an employee or agent:

- First, the employee or agent must have committed a criminal act within the scope of his or her authority with the corporation.
- Second, the employee or agent must have acted with the intent, at least in part, to benefit the corporation.

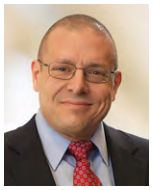
Q8. At what point does liability shift between employee and employer? And what measures should businesses incorporate to counteract the increasing regulatory compliance burden?

Jodi Avergun

Similarly, under the Supreme Court-created Responsible Corporate Officer (RCO) doctrine, a corporate officer may be found criminally liable for regulatory offenses even when he or she is unaware of and not involved in the wrongdoing if he or she is in a position of authority regarding the activities giving rise to the illegal conduct and failed to prevent or correct the conduct. *United States v. Park*, 421 U.S. 658, 672–74 (1975); *United States v. Dotterweich*, 320 U.S. 277, 284–85 (1943). Penalties under the RCO doctrine can include fines and imprisonment. *Meyer v. Holley*, 537 U.S. 280, 287 (2003).

Although by no means a guarantee, the best way for a business to insulate itself from being held liable for the acts of its employees is to have a comprehensive compliance program that accurately and adequately assesses risk, and that is communicated to company employees in a meaningful way. This generally entails thorough written policies delineating acceptable conduct, periodic training, financial incentives for compliance, and appropriate whistle-blower policies.

Q9. How can companies ensure they get the balance right between implementing risk management and risk prevention?



Salvatore LaScala

(i) Risk Management:
Effective risk management means that senior management makes deliberate decisions to understand, accept, and mitigate identified risks. As a side note, it's important to recognise that risks change as the organisation changes — thus organisations should have a process in place to identify and address the revised risk profile. This requires resources, commitment, and authority given to responsible individuals. Once the risks are identified, organisations need to institute controls to help mitigate and manage the risk. Communicating the risk strategy broadly, collaborating between all departments of an organisation, and identifying and reporting on emerging risks are essential for understanding the risks and accurately disseminating the information so relevant stakeholders are able to manage these risks.

(ii) Risk Prevention:
Risk prevention means the act or practice of stopping something bad from happening. Risk prevention methods include comprehensive policies, procedures, processes, and controls that are designed to prevent and detect illegal or unethical conduct. Each organisation should tailor relevant industry best practices and risk prevention methods to fit its needs. This may include limiting the products it offers or geographies in which it is willing to do business. It might include deciding not to accept certain types of clients.

(iii) Risk Balance:
Companies can ensure the right balance between risk management and risk prevention by identifying risks and determining how much risk they are willing to tolerate. Senior management must set its risk appetite based on a careful analysis of various factors, including the following:

- Regulatory impact
- Consumer impact
- Reputational impact
- Existence of an enforcement action, (i.e., consent order, Deferred Prosecution Agreement)
- Financial reward impact

Senior management can then manage the risk by either eliminating it — cutting ties with certain customers — or by managing it with an adequate control environment. Risk management and risk prevention share the same goal: reduce the organisation's risk, loss, and liability exposure.

Q10. Can you talk us through the various steps a company should take upon discovering fraud?

Tobias Eggers

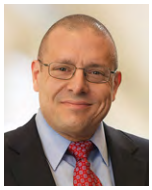
The first steps would be to:

- Determine the gravity of the offence from an outsiders' perspective (publicity) and from an economic standpoint (how much money did/will you lose?).
- Determine the likelihood of other offences (fraud more often than not is not a singular event and if one employee is involved there may be others)
- Determine the likelihood of the information being uncovered by third parties (press, prosecutors, authorities, competitors, former employees)
- Determine the importance of the employee or business partner involved.
- When will the statute of limitation run out? Is waiting an option?
- Do you have an obligation to make a complaint (i. e.: tax fraud)?

Having considered this: Decide if you conduct an internal investigation yourself (you will have all the information and will not have authorities poke around in your company; you will stir things up in your company). Talk to your lawyers about this.

Other things to think about: Can you access the email account of the perpetrator? Are you allowed to do so? Where will the results of the investigation be safely stored? Who would be the people you should confront first? How can you keep it low profile? Can you make your employees speak to you? Ramifications if you have to fire one of them?

Having all the information: Decide if you make a public criminal complaint – and go to the press, too. If it is unavoidable that the prosecution will get knowledge of the offence and will turn your company upside down: Act first; do not wait for them. Feed them the information in a way that is best for you.



Salvatore LaScala

The availability of reduced penalties for cooperation and the increased number of whistleblowers create incentives for companies to be proactive in assessing and investigating potential allegations of illegal or unethical conduct.

Of course, the key step in the investigation process is to ensure that the organisation has developed and implemented an effective and comprehensive corporate compliance program to prevent and detect such conduct. In other words, the best offence is a good defence.

Because no compliance program is perfect (and regulators don't expect compliance programs to prevent and detect every instance of illegal or unethical conduct), an effective compliance program should recognise that there may be a need to conduct investigations into potential wrongdoing and should also contain an employee whistleblower program that allows employees to anonymously report any potentially illegal or unethical activity. The compliance program should include documented internal investigation protocols that address matters including, but not limited to, preservation, collection, and analysis of documents; preparing for and conducting employee interviews; internal and external communications regarding the matters; when to retain outside counsel, and investigative and forensic experts; and considerations for making voluntary disclosures to the government.

"Because no compliance program is perfec, an effective compliance program should recognise that there may be a need to conduct investigations into potential wrongdoing and should also contain an employee whistleblower program that allows employees to anonymously report any potentially illegal or unethical activity."
- Salvatore LaScala -

Q10. Can you talk us through the various steps a company should take upon discovering fraud?

Angela Barkhouse

The immediate steps I would advise are the following:

i. Ensure you preserve potential evidence. The proper extraction of key documentation is crucial, including digital information. The system for handling documents must always be a primary concern, particularly digital or electronic evidence, as it can be easily altered or destroyed if incorrectly handled, leading to the possibility that the material is inadmissible in legal proceedings as its authenticity cannot be verified. This careful approach applies equally if not more so when obtaining digital evidence. The forensic approach towards a computer in a standalone environment is very different from that on an IT network administrator. Although tempting, one should avoid directly examining or using the suspect's computer. Browsing and opening files from a suspect's computer can be devastating, as it will contaminate critical evidence such as the date and time stamp. It can also trigger any destructive commands implanted by the suspect. Such damage can be permanent and irreversible and destroy evidence that could have led to a successful prosecution. Maintaining the evidence will help your forensic accounting team identify what occurred, who committed the fraud and why.

ii. Retain professional advisors. Enlist a forensic accountant and computer forensic specialist to help you collect, analyse and store the data. A forensic examination of evidence to support a prosecution or civil claim is not the same as a financial audit. They differ in terms of objective, scope, methodology, and training. A financial audit aims to provide the reader of the financial statements reasonable assurance that the financial statements are free from material misstatement. Auditors will be trained in the required standards for financial reporting, whilst forensic accountants and financial investigators will have had training in the investigation and litigation process. Retain a lawyer who has professional expertise in fraud litigation. I once had to work with a lawyer who had been retained prior to my engagement whose professional expertise was in construction but who was well known to the firm. Needless to say, it was a frustrating and lengthy process which was quite unnecessary.

iii. File any potential loss with your insurer. You may need to document any losses with your insurance provider in a specified time frame and/or take specific actions in order to comply with certain provisions.

Pursuant to the above, and in conjunction with its professional advisors, the company will be able to work out the most appropriate and effective strategy for mitigating and recovering any losses, and understanding the extent to which further action may be needed; whether it is submitting a criminal complaint, or taking steps to file legal proceedings, mitigate reputational damage via public relations or resolving operational/control risks.

Craig Weston

The very short and succinct answer is to take a step back and properly plan and next steps. Generally in the UK we would advocate taking the following steps in the following order to help ensure the most effective internal investigation and also to protect the business:

- Set up an small investigation team and empower them to seek and receive legal advice by way of a board resolution;
- Give the investigation a Project Name;
- Consider and define the scope of the investigation;
- Create an email group for the project team;
- Consider the instruction of external legal advisers;
- Communicate to all team members that the matter should remain confidential and not be discussed outside of the project team;
- Preserve evidence – get your IT team to image servers, ensure the document retention policy is suspended and order no documents to be destroyed.

Q10. Can you talk us through the various steps a company should take upon discovering fraud?

Craig Weston

To help maintain privilege over the internal investigation for proceedings that may flow from the conduct, use your in-house lawyer in their capacity as an in-house lawyer or external lawyers to assist in key parts of the investigation:

Planning and conducting internal interviews with employees;
Instructing experts such as auditors or forensic accountants;
Advising the board on potential outcomes;
Identify a list of people and document you need to speak to and review;
Consider if you are regulated and whether there is a reporting obligation to the regulator based on the uncovered conduct;
Keep a documented audit trail of key decisions such as scope of the investigation, selection of employees and documents to speak to/review;
Do not be quick to jump to conclusions.

Jodi Avergun

A company has numerous decisions and actions to take upon discovering fraud. Most importantly, a company needs to evaluate whether or not to make a voluntary and full disclosure to criminal prosecutors or regulators. Whether or not disclosure is ultimately made, companies are well-advised to take the following steps early in the matter:

i. Consider how to investigate the allegation and who will conduct the investigation. If the investigation is conducted by in-house auditors, or even in-house counsel, it is less likely to be protected by attorney client and attorney work product privilege than if the company engages outside counsel.

ii. Issue clear but measured document hold notices to key employees and their administrative assistants. Ensure that hold notices extend to all media and personal as well as work devices.

iii. Identify key witnesses to interview and key documents to review.

iv. Obtain independent counsel for key witnesses where appropriate and necessary, but not before corporate counsel has a chance to interview the employee.

v. In collecting documents, be mindful of strict data privacy and data-sharing statutes, particularly the new GDPR and strict privacy regimes like France.

vi. Identify the root cause of the misconduct and start remediating the error. If necessary, discipline up to and including firing culpable employees must be considered.

vii. Consider whether company policies adequately addressed the misconduct, and if so, whether those policies were circumvented.

viii. Consider how to document witness interviews, as well as preservation and collection steps.

ix. Prepare presentations for company board and ultimately, regulators, about the discovery of the misconduct and the remedial measures taken to address the misconduct.

x. Assess, with assistance from forensic investigators, financial impact of misconduct.

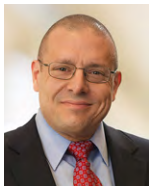
Q11. To what extent has whistleblowing and self-reporting incentives changed the way companies manage and respond to fraud?

Tobias Eggers

Germany for quite some time did not have any legal whistle blowing framework at all. This is, studies say, – still – due to the fact that it reminded people of snitches during the Nazi regime as well as the very elaborate informant system in the GDR. Companies to this day will oftentimes not appreciate when you ask them to implement a whistle blower hotline.

However, times are changing and we see that these measures work in other countries. The idea though, that you would get a reward for snitching on your colleagues (US and other countries) still does not seem palatable for many businesses. Companies are introducing whistle blower systems (call them differently, though) these days. Those who do, though, hardly connect whistle blowing to any reward. Instead they are trying to (compliance) speak to an inner responsibility of the employees who are to protect their company and their fellow employees. You can imagine that this works for some people better than for others.

Whistle blower hotlines, if they exist within companies (most of the big ones have some sort of system), are seldom used, though. It will still take some time until the German aversion against whistle blowing goes away. One can regret this but this is the state of the game.



Salvatore LaScala

There are various U.S. whistleblower statutes, rules, and regulations, including Section 922 of the Dodd-Frank Act and the False Claims Act. Generally, these regulations allow financial rewards to individuals who provide information which results in a successful enforcement action or prosecution against a wrongdoer. To encourage the free flow of information regarding potentially illegal activities, whistleblowers are also provided with anonymity, and federal law prohibits retaliation against them for providing such information.

Since the advent of the SEC whistleblower program, more than 14,000 whistleblower tips from all 50 states and 95 foreign countries have been received and significant financial rewards have been paid out. More than $168 million was paid to 13 individuals in 2018 alone. In addition to the U.S., comprehensive whistleblower protection laws have been adopted in more than a dozen countries and several other countries provide more limited protections. The pace of whistleblowing is only going to increase as more whistleblower payments are made and publicised and whistleblowing is viewed more and more as a potentially lucrative activity.

The increased number of whistleblower complaints and payments has required companies to react to and address whistleblower allegations more quickly. This trend has also forced companies to consider the need for voluntary disclosure to the government to admit wrongdoing before whistleblowers call attention to it.

Q11. To what extent has whistleblowing and self-reporting incentives changed the way companies manage and respond to fraud?

Esra Bicen

Turkish Penal Code article 278 defines failure to disclose a criminal activity as a primary offence with penalty of imprisonment. Although this approach to whistleblowing seems far more advanced compared to incentives created under the 2010 Dodd-Frank Act and 2018 EU Directive on the Protection of the Persons Reporting on Breaches of Union Law, Turkish Penal Code does not have a provision to protect the identity of the whistleblower. Knowing that they cannot stay anonymous, it is almost impossible for whistleblowers to come forward and disclose any corporate or financial wrongdoing facing the risk of serious retaliation in their companies and blacklisting in the industry. Turkish Penal Code also fails to give financial rewards to whistleblowers such as the Dodd-Frank "bounty program", which is another deterrent for a whistleblower facing the risk of losing his/her job.

In addition, Turkish Penal Code article 278 does not make a distinction as to the true intent of the whistleblower. In a recent highly publicised case resembling Edward Snowden's leaking of US National Security Agency's illegal surveillance techniques to the American public, two Turkish journalists were prosecuted for disclosing information regarding arms trafficking in trucks belonging to the National Intelligence Agency. This case opened a hot debate about whistleblowing on government agencies and as to whether the intent of the whistleblower should matter unless such intent satisfies the elements of another primary offence which then gives reasonable ground for his prosecution.

Q12. What options exist for companies to investigate the fraud and recover the proceeds in cross-border fraud or misconduct?

Tobias Eggers

Being a victim company usually gives you the benefit of not having to think about whether you open up about it to the prosecutor. That means – in most cases – that you will be able to get the investigative power and asset seizure power of the government behind you.

However, cross border freeze and asset recovery for most prosecutors is not seen as their primary goal. The reason for that being they do not care if you get your money back. They just need to get the bad guys. However, if the perpetrator has more assets than you will be able to reclaim, they might get some part of the crime's proceeds. It is therefore worthwhile to try and bring the prosecution to investigate, using their considerable powers.

In cross border cases it is worth noticing that the amount of money currently being recovered in the EU is only a small proportion of estimated criminal proceeds: 98.9% of estimated criminal profits are not confiscated and remain at the disposal of criminals (Europol Survey). Therefore it will also be best, not to just rely on the prosecution to follow and claim your money but to engage with competent lawyers in the countries the perpetrator invested in.

These two approaches go hand in hand. Prosecution, for instance, will be able to give you access to bank statements of the accused. Through this you should be able to determine where he sent his money to. In those countries you will have to rely on local legal counsel.

In 2016, according to Europol Data, 2.2% of the estimated proceeds of crime were provisionally seized or frozen, however only 1.1% of the criminal profits were finally confiscated at EU level. That means that around 50% of all provisionally seized/frozen assets were ultimately confiscated. EU countries are currently aligning their national legislations with the EU Directive on the freezing and confiscation of proceeds of crime.

Most countries have a conviction based confiscation regime in place. The majority of EU Member States also stated that they are implementing an extended confiscation regime or a non-conviction based approach. This means that you will not have to wait for a conviction before you get your money back.

Q12. What options exist for companies to investigate the fraud and recover the proceeds in cross-border fraud or misconduct?

Tobias Eggers

In Germany the last two years have seen fundamental change in the asset recovery framework. It is getting easier to make prosecution go after the accused for your money.

Angela Barkhouse

Complex frauds are often multi-jurisdictional, therefore understanding international legal remedies is key in determining a successful strategy.

We use a range of remedies depending on the most efficient route to recovery. For example, we may use insolvency tools if there is debt owed, and in some fraud causes it may be possible to obtain a winding-up or receivership of a person or legal entity which could provide additional discovery powers regarding assets, and possibly additional causes of action to be pursued. Private civil action seeking damages for breach of trust, or negligence may be more appropriate depending on the evidence, involvement of third parties, and jurisdictional nexus.

We have heard many times from litigants pursuing claims (and maybe even having successful judgements) that they made no recoveries of assets. Too often we hear stories of wasted money and time spent pursuing a remedy that was not viable, or worse obtaining a judgement but failing to bring in a recovery. It is important not just to take action, but to ensure that the assets exist at all. We have come across one or two cases where our investigations identified that the money had been frittered away and that pursuit of recovery was not worthwhile. That is not to say however that a criminal complaint should not be pursued in parallel, and evidence obtained can support these too. It is critical, therefore, that you do some research upfront to ensure those advising you, particularly offshore, have the relevant knowledge and experience to get you the best result.

Esra Bicen

The answer depends on who commits the fraud in a company. If the wrongdoer is the board itself, then it will not be possible to engage the board in retaining a private forensic expert to conduct a special audit to disclose the scope of the fraud. In such cases, any shareholder may request intervention of the Commercial Court of First Instance to by-pass the board to order an investigation regarding a wrongdoing in the company.

Recovering proceeds of cross-border misconduct depends on obtaining a final judgment against the wrongdoer in one jurisdiction, locating assets/proceeds of the wrongdoer in Turkish jurisdiction and obtaining an enforcement judgement "exequatur" in Turkey to seize those assets/proceeds. The Act on Private International Law and International Procedural Law (PILA) allows enforcing a foreign judgement in Turkey provided that an agreement to enforce judgments rendered in both jurisdictions or a de facto reciprocity to this effect exits, no judicial exclusivity applies to the subject matter of the dispute in Turkey and the foreign judgment is in line with the Turkish public order. As long as the above conditions of the PILA are satisfied a petition can be filed before the Commercial Court of First Instance to request an enforcement judgement.

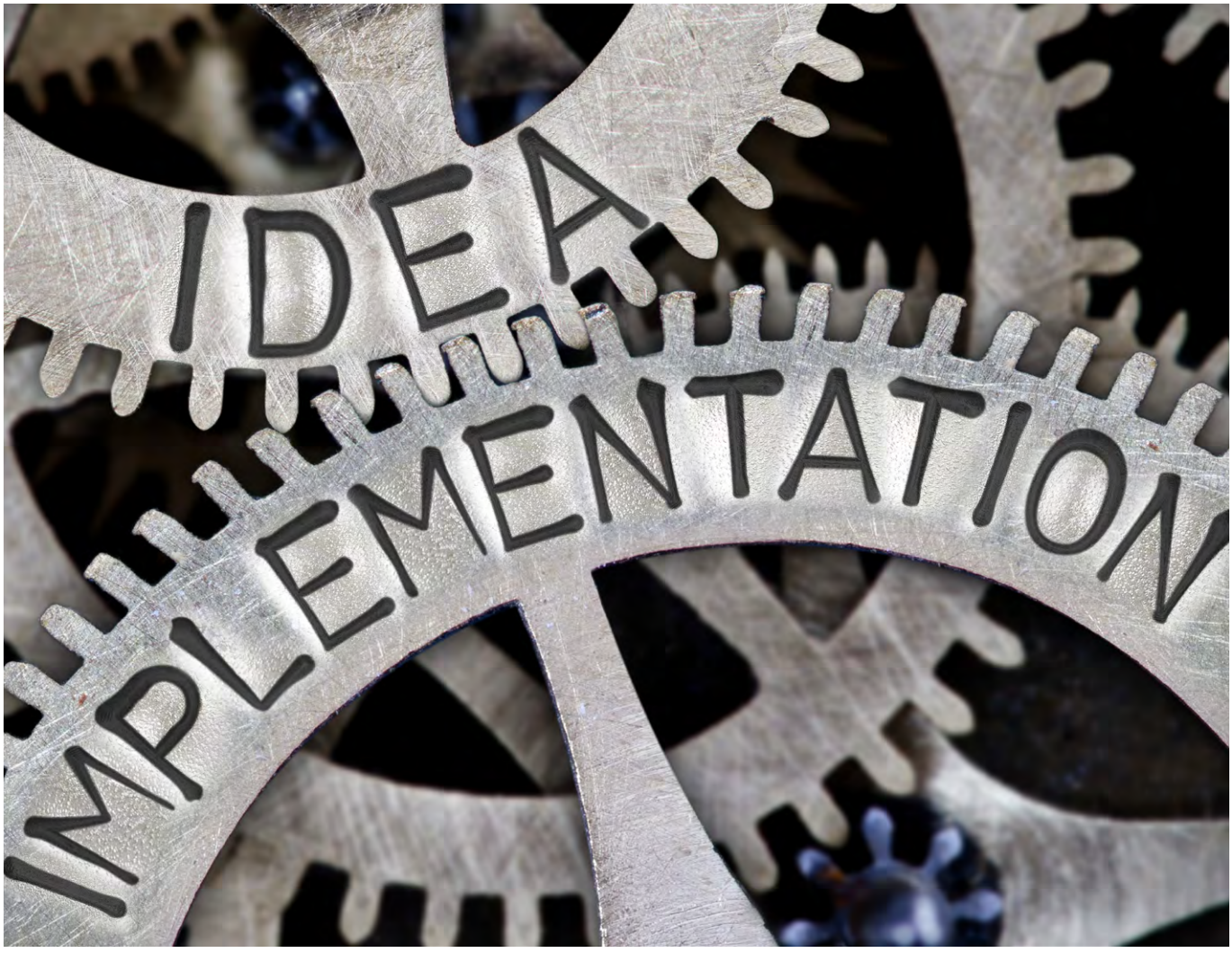
Q13. In an ideal world what would you like to see implemented or changed?

Dennis Miralis

It is hoped that more effective frameworks will be developed in the area of global cyber- crime reporting and investigations. Government's worldwide need to ensure that they implement effective education campaigns to protect their citizens from internet fraud and to improve the ways in which cybercrimes frauds are investigated.

Craig Weston

Extension of failing to prevent to other offences – driving up industry standards and conduct – funding investigatory and prosecutorial bodies to investigate other crimes more effectively.



CorporateLiveWire