The Fraud & White Collar Crime 2020 Roundtable discusses recent developments in the legislation and enforcement of corporate fraud, bribery, corruption, tax evasion and insider trading. Other notable topics include: the prominent bribery case U.S. v. Hoskins, cross border investigations, the agencies tackling corporate misconduct and the effects of Brexit on white collar crime efforts.

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?

Q2. Have there been any recent regulatory changes or interesting developments?

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

Q4. Can you outline the key fraud & white collar crime trends?

Q5. How about compliance and enforcement trends?

Q6. Which government agencies investigate fraud & white collar crime?

Q7. How are cross border investigations conducted?

Q8. Can you outline the best practice for corporate governance and internal control considerations?

Q9. What steps should a company should take upon discovering fraud?

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

Introduction & Contents

The Fraud & White Collar Crime 2020 Roundtable discusses recent developments in the legislation and enforcement of corporate fraud, bribery, corruption, tax evasion and insider trading. Other notable topics include: the prominent bribery case U.S. v. Hoskins, cross border investigations, the agencies tackling corporate misconduct and the effects of Brexit on white collar crime efforts.

Meet The Experts

Ravinder Thukral - Brown Rudnick LLP
T: +44 (0)20 7851 6063
E: rthukral@brownrudnick.com

Ravinder Thukral is one of the award-winning 14 litigation and arbitration partners in the London office of Brown Rudnick LLP, which combines cross-border civil fraud, criminal and regulatory expertise under one roof. He has particular experience of banking and finance, civil fraud, shareholder and real estate disputes both in the UK, the Middle East and India. He also advises individuals and companies facing criminal investigation or prosecution by major enforcement bodies. He has experience as a criminal prosecutor and has represented those accused of fraud, bribery and money laundering.

Peter Binning - Corker Binning
T: +44 (0) 20 7353 6000
E: pbin@corkerbinning.com

Peter Binning is a highly respected criminal defence lawyer who specialises in fraud and regulatory litigation. He has many years’ experience of investigations and prosecutions relating to fraud, regulatory breaches, corruption, cartels, export control, sanctions and tax evasion.

Peter previously worked as a prosecutor for the CPS and the SFO before becoming a partner at Peters & Peters. He co-founded leading crime and regulatory firm Corker Binning Solicitors in 2001. Peter is ranked as a top tier lawyer in Chambers UK and Legal 500, and recognised as the leading English practitioner of Business Crime Defence by Who’s Who Legal 2014.

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

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

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

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

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

Timothy Le Cornu - KRyS Global
T: +44 1481 711 211
E: timothy.lecornu@krys-global.com

A steady hand with 25 years of experience in some difficult areas of the world, Tim has proven himself on countless occasions in complex and challenging situations. Known for getting to the heart of the issue quickly, while earning the trust of his client, he’s the professional who’s not scared to ask the hard questions and work towards a practical solution. He has an exceptional ability to cut through any tensions or disputes, identify core issues and find ways to bring value to clients.
Ryan Junck is a partner in Skadden’s European Government Enforcement and White Collar Crime practice, representing corporations and individuals in criminal and civil matters in federal and state courts. He has extensive experience in conducting internal investigations and U.S. and multinational regulatory investigations, including those brought by the DOJ, SEC, OFAC, Federal Reserve and U.S. Congress, and various international regulators.

Mr. Junck also has substantial experience representing clients in cross-border matters, including investigations concerning insider trading, financial fraud, the FCPA and economic sanctions laws. He is ranked in Chambers UK, was named a Transatlantic Rising Star at the 2016 American Lawyer Transatlantic Legal Awards, and was one of Global Investigations Review’s 2017 40 Under 40.

Michael Ruck is a partner in TLT’s financial services team in London and a member of our Investigations team, which supports clients on sensitive reputational matters and investigations.

Michael previously spent four and a half years at another City law firm in the corporate crime, investigations and enforcement team and before that spent almost six years working in the FCA’s Enforcement and Market Oversight Division. Michael is a highly experienced investigations lawyer.

He has a broad range of experience including advisory, regulatory liaison and large-scale, complex multi-jurisdictional investigations. He has led financial services regulatory projects, investigations and proceedings for a range of institutions, including asset and fund managers, insurance businesses and banks. His experience spans various regulatory issues and he has worked closely with a number of UK and foreign regulators, including the FCA, SFQ, ICO, DJJ and IRS.

Michael has a deep understanding of a wide range of regulatory issues and procedures, making him a trusted adviser to his clients, often at board level.

Dennis Miralis is a leading Australian lawyer who acts and advises in complex international cyber crime investigations and prosecutions involving some of the world’s largest law enforcement agencies and regulators, including the FBI, Europol and the Australian Federal Police.

Dennis also conducts complex international cyber investigations on behalf of companies and individuals who are victims of cybercrime, including identifying the proceeds of crime in offshore locations and assisting with asset recovery and international investigations.

He advises companies that are subject to data breach reporting requirements under Australian law and specialises in extradition, mutual legal assistance and Interpol related matters regarding cyber crime. Dennis has extensive experience in high stakes complex cases intersecting international security law and cyber crime.
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?

Ruck: UK legislation in relation to corporate fraud, bribery and insider dealing has grown significantly in both number and reach over recent years.

i. **Fraud**

Section 1 of the UK Fraud Act 2006 created three fraud offences of fraud by false representation, fraud by failing to disclose information and fraud by abuse of position.

ii. **Bribery and corruption**

The UK Bribery Act 2010 came into force on 1 July 2011 and remains the key legislation for general bribery offences, including the corporate offence of failing to prevent bribery (section 7). The SFO issued revised statements of policy in October 2012 covering facilitation payments, hospitality and gifts, and self-reporting.

iii. **Tax evasion**

The Criminal Finances Act 2017 includes a similar corporate offence to that in the Bribery Act, namely the corporate offence of failing to prevent the facilitation of tax evasion.

iv. **Insider dealing**

The Criminal Justice Act 1993 (Part V) (CJA) contains the criminal offence of insider dealing. Part 7 of the Financial Services Act 2012 (FSA Act 2012) contains the criminal offences of making false or misleading statements, creating false or misleading impressions, and making false or misleading statements or creating a false or misleading impression in relation to specified benchmarks. The FSA Act 2012 repealed section 397, Financial Services and Markets Act 2000 (FSMA) with effect from 1 April 2013. Section 397, FSMA previously prohibited misleading statements and market manipulation.

The Market Abuse Regulation (Regulation 596/2014) (MAR) as implemented in the UK repealed and replaced the Market Abuse Directive with effect from 3 July 2016.

MAR contains a completely separate civil offence of insider dealing to the criminal offence covered in the CJA. MAR also contains the civil offences of unlawful disclosure of inside information and market manipulation.

The FCA has issued guidance on MAR in its *Market Conduct Sourcebook*, including examples of behaviour which may amount to contravention of each of the civil offences.

Poston: (i) **Fraud**

In my jurisdiction, the Southern District of Florida, which includes Key West north to Ft. Pierce, Florida, the focus is not so much on corporate or business fraud, but more on FCPA and money laundering prosecutions, with a particular focus on the oil and gas industry in South America. One of the largest money laundering cases ever filed by the DOJ practice is customary in the industry, trade, business, or profession is no defence to these crimes.

(ii) **Bribery and corruption**

A similar set of FCPA and money laundering cases have focused on Petroecuador, Ecuador’s nationally-owned oil and gas company. These FCPA cases are managed by the FCPA unit in Miami, along with the FCPA unit in the Criminal Division of Main Justice, in D.C. So far, those defendants apprehended have all pled guilty, been assessed personal money judgments.

(iii) **Insider trading**

Although not in my District, one should mention the recent Second Circuit ruling that looks to make it easier for federal prosecutors to obtain convictions for insider trading.

Under the 1985 U.S. Supreme Court decision in *Dirks v. Securities and Exchange Commission*, 1 prosecutors have had to prove that insiders received some “personal benefit” in exchange for the tips they passed to traders.

A three-judge panel in the case of U.S. v. Blaszczak, 2 rejected the argument that 35 years of rulings in insider trading cases brought under Title 15 of the U.S. Code, Exchange Act, should apply to cases brought under the newer securities fraud statute, 18 U.S.C. Sec. 1348.

Blaszczak argued that the more intricate rules under the Exchange Act should apply equally to cases brought under Title 18 securities fraud.

The Second Circuit rejected the defendant’s argument and declined to graft the Dirks personal benefit test onto the elements of 18 U.S.C. Sec. 1348.

This decision comes on the heels of the House of Representatives passing a bill meant to address the lack of a law explicitly banning insider trading. There is more to come on this topic as a working group led by Katherine Goldstein, a former head of the Securities and Commodities Fraud Task Force at the U.S. Attorney’s Office in Manhattan, is preparing to issue its own recommendations on insider trading to Congress and the SEC.

Miralis: (i) **Corporate or business fraud**

Part 4AA of the New South Wales Crimes Act sets out offences related to fraud and fraudulent statements, fraudulent destruction or concealing of accounting records, and deceiving members or creditors by false or misleading statements by an officer of an organisation. Part 4C sets out provisions related to money laundering offences. Part 5 contains provisions relating to forgery offences. All these offences can be committed by both natural persons and corporate entities.

(ii) **Bribery and corruption**

In terms of New South Wales law, bribery and corruption offences are dealt with in Part 4A of the Crimes Act. These offences include corruptly obtaining commissions or rewards, the provision of misleading documents by an agent to their principal, corrupt inducements for advice, and the receipt of corrupt benefits. An argument that the alleged practice is customary in the industry, trade, business, or profession is no defence to these crimes.

---

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?

The Commonwealth Criminal Code also contains a number of provisions relating to bribery offences. In particular, section 70.2 sets out the offence of bribing a foreign public official, and Divisions 141 and 142 contain offences related to bribery of Commonwealth public officials.

(iii) Insider Trading

Part 7.10, Division 3, of the Commonwealth Corporations Act contains extensive provisions related to prohibitions on insider trading. Essentially, these provisions prescribe that a person in possession of insider information from gaining or procuring another to gain financial products relevant to that information. Contravention of these laws may result in criminal prosecutions or the imposition of civil penalties.

Le Cornu: Guernsey has a well-developed body of laws to regulate the activities of its financial services sector which is the largest part of the Island’s economy and is therefore crucial to the future of the Island’s welfare. Many of those laws will cross over the three categories identified.

Corporate or Business Fraud

- The Companies (Guernsey) Law (2008)
- The Fraud (Bailiwick of Guernsey) Law, 2009
- The Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2001
- The Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law, 1991
- The Criminal Justice (International Co-operation) (Enforcement of Overseas Forfeiture Orders) (Bailiwick of Guernsey) Ordinance, 2007

Bribery and Corruption

- The Prevention of Corruption (Bailiwick of Guernsey) Law, 2003
- The Handbook on Countering Financial Crime and Terrorist Financing (“the Handbook”)
- The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999
- The Protection of Investors (Bailiwick of Guernsey) Law, 1987 (“POI Law”)
- The Criminal Justice (Abductions and Abetting etc.) (Bailiwick of Guernsey) Law 2007

Insider Trading

- The Company Securities (Insider Dealing) (Bailiwick of Guernsey) Law, 1996, as amended
- The Code of Market Conduct (prepared and issued under Section 418 of the POI Law)
- Insider Dealing (Securities and Regulated Markets) Order, 1996
- Insider Dealing (Securities and Regulated Markets) Amendment Order, 2017
- Protection of Investors (Market Abuse) (Bailiwick of Guernsey) Regulations, 2008

The list above is not exhaustive and there are many other laws which cover a range of offences from drug trafficking, counterfeiting, terrorism, conspiracy and forfeiture of property.

In addition, regular Guidance Notes and Instructions for Financial Services Businesses and Prescribed Businesses are prepared and distributed by the Guernsey Financial Services Commission (“GFSC”) in relation to developments in countering and detecting financial crime. The International Stock Exchange requires its members to comply with its own regulations in conducting business with investors including provisions related to insider trading and market manipulation. All financial services businesses and prescribed businesses are required to submit a Financial Crime Risk

Q2. Have there been any recent regulatory changes or interesting developments?

Thukral: Following the publication of a section of the SFO’s “Corporate Co-operation Guidance” (part of the SFO’s Operational Handbook) in 2019, the SFO has maintained its drive towards greater openness and transparency with the recent publication (in January 2020) of its internal guidance on Evaluating a Compliance Programme.

This eight-page document makes clear that it is for internal guidance and not for the purpose of providing legal advice. That being so, the document explains that the SFO’s assessment of a compliance programme is relevant to the SFO’s decisions on, inter alia, whether a corporate should be prosecuted; whether it should be invited to DPA negotiations; whether the corporate has a defence of “adequate procedures” to a charge of failing to prevent bribery under section 7 of the Bribery Act 2010 and sentencing. In particular, the document makes clear that the SFO’s investigation teams should explore compliance issues early in the investigation. It then repeats the “Six Principles” identified in the 2011 Guidance issued by the Ministry of Justice under the Bribery Act as representing “a good general framework for assessing compliance programmes”.

While it is helpful to see the continued adoption of these principles by the SFO (namely, proportionate procedures, top level commitment, risk assessment, due diligence, communication, and monitoring and review) they do not provide any obviously new assistance to corporates who may wish to update or improve their compliance programmes. When compared to their U.S. equivalent, they also lack the level of detail set out by the U.S. Department of Justice in its publication, Evaluation of Corporate Compliance Programs which remain a useful benchmark to corporates everywhere.
Q2. Have there been any recent regulatory changes or interesting developments?

Poston: I would say in 2019, the U.S. regulatory developments and enforcement regarding OFAC sanctions exploded. Not only did U.S. Treasury’s OFAC strengthen its existing sanctions against Venezuela and Cuba, OFAC also published its expectations for its sanctions compliance programme and expanded the scope of sanctions-related reporting requirements for U.S. persons. Let me address these one at a time.

Compliance Program Guidance Overview

This OFAC guidance states that “each [sanctions compliance] program should be predicated on and incorporate at least five essential components of compliance: (i) management commitment; (ii) risk assessment; (iii) internal controls; (iv) testing and auditing; and (v) training.” These five pillars track the compliance undertakings that OFAC has incorporated in its recent settlement agreements.

However, the document clarifies that OFAC “strongly encourages” companies — including non-U.S. companies that may be subject to U.S. jurisdiction solely by virtue of their dealings with U.S. counterparties or U.S.-origin goods, services or technology — to adopt formal compliance programs. This guidance confirms that OFAC has significantly escalated its compliance programme expectations. As with the publication of the DOJ’s and the Securities and Exchange Commission’s Resource Guide to the U.S. Foreign Corrupt Practices Act, published in 2012, OFAC’s guidance is likely to be viewed as a key benchmark against which sanctions compliance programmes will be measured going forward.

Sanctions-Related Reporting Requirements for U.S. Persons

All U.S. persons must now inform OFAC of any “rejected transactions,” which the agency defined in the interim final rule as “wire transfers, trade finance, securities, checks, foreign exchange, and goods or services.”

A different provision, 603 of the same section, mandates lenders to report and block all transactions directly involving individuals or entities whose names appear on the U.S. list of “Specially Designated Nationals,” or SDNs, by placing the related funds in a separate account and holding them.

While there is no change to the activity that is prohibited, the scope of what activity has to be reported has expanded. Following the amendments, non-financial businesses — for example shipping, trading and technology firms, previously excluded by the rule — must now also submit reports to OFAC when they reject “a transaction that is not blocked” but that “would nonetheless violate” U.S. sanctions. This requires incredible diligence when it comes to monitoring the sanctions issued by OFAC and the amendments thereto.

Miralis: In late 2019, the Federal Government introduced the Crimes Legislation Amendment (Combating Corporate Crime) Bill to Parliament. If passed, this legislation will increase law enforcement scrutiny on the overseas activities of Australian companies, particularly in respect of foreign bribery.

A cornerstone of the Bill is the newly created corporate offence of failing to prevent foreign bribery. This will significantly increase the scrutiny on the robustness of internal anti-bribery and corruption mechanisms as companies will be held criminally responsible for foreign bribery committed by employees, external contractors, agents and subsidiaries unless “adequate procedures” to minimise the risk were in place.

This offence will carry a maximum penalty of the greater of $21 million, 10% of the offending company’s annual turnover, or three times the benefit gained from the underlying illicit activity.

Le Cornu: In December 2018, the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance 2018 (“Ordinance”) was passed to bring Guernsey’s framework for combatting money laundering and financing terrorism into line with the Financial Action Task Force standards issued in 2012. The Ordinance also addressed certain recommendations made by MONEYVAL1 in its report issued in January 2016.

During 2018, the GFSC updated the Handbook which included extensive consultation with the island’s financial services industry. The Handbook was issued by the GFSC on 12 March 2019 and came into effect on 31 March 2019, and replaced the previous two handbooks for financial services businesses and prescribed businesses (lawyers, accountants and real estate agents) to reduce duplication.

The GFSC conducted education programmes of the revised framework during 2019 with regulatory self-assurance workshops to aid the finance industry in complying with the new rules.

Keenan: Enforcement of corruption laws and regulations continues to dominate with large scale settlements announced in an increasing number of international jurisdictions. There are also a growing number of prosecutions involving U.S. sanctions and export control violations, which is perhaps unsurprising given the press scrutiny on international trade. The DoJ has continued their increased focus on holding individuals accountable for misconduct, in addition to corporations.

2019 saw an increased number of charges brought by the Criminal Division’s FCPA Unit against individuals, with more guilty pleas than ever before. Three of the recent FCPA-related jury trials, which are rare in themselves, ended in the convictions of defendants. DOJ’s Assistant AG Brian Benczkowski stated in early December 2019 that “the Criminal Division’s FCPA Unit has publicly announced more charges against individuals [34] than in any other year in history. It has also publicly announced more guilty pleas by individuals [30] than ever before.”

Another interesting development as it relates to FCPA enforcement involved the announcement by Glencore, one of the world’s largest commodity traders, that it is being investigated by the Commodity Futures Trading Commission (CFTC), for possible corrupt practices. This represents a new enforcement agency in this arena, previously the domain of the DOJ and SEC.

In the UK, attention is directed towards the role the audit profession has played with several large corporate failures, including some involving inappropriate accounting. If there is an economic downturn, these cases may increase and continue the discussion within the UK government as to how to address apparent audit failures. In the U.S., there remains a stream of accounting fraud cases involving revenue recognition and earnings management, but nothing on the scale of accounting failures witnessed at the start of the century.

1. A permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems.

“In late 2019, the Federal Government introduced the Crimes Legislation Amendment (Combating Corporate Crime) Bill to Parliament. If passed, this legislation will increase law enforcement scrutiny on the overseas activities of Australian companies, particularly in respect of foreign bribery.”

- Dennis Miralis -
Q2. Have there been any recent regulatory changes or interesting developments?

Junnck: One interesting development of 2019 in the enforcement sphere is the ways in which economic sanctions enforcement is increasingly used as a key instrument of U.S. foreign policy, and how enforcement activities have increased in parallel.

The Trump Administration has launched maximum pressure campaigns against Iran and North Korea, and made substantial and repeated changes in the past few years to sanctions against Russia, Iran, North Korea, Venezuela, Cuba, Myanmar (Burma), and Sudan. We have also witnessed the Administration targeting larger entities with the Office of the Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) sanctions (such as Russia’s GAZ Group in April 2018), and demonstrating a greater willingness to use new models of sanctions as political tools (such as the sanctions imposed on Venezuela’s PDVSA in January 2019).

The Administration’s focus on sanctions enforcement was further typified when, on 27 November 2019, President Trump signed two bills into law that increased U.S. sanctions and export control restrictions towards China, in direct response to the recent crackdown on political protests in Hong Kong. Though not strictly sanctions enforcement, in October 2019 the U.S. Commerce Department placed 28 Chinese public security bureaus and companies (including 19 subordinate government agencies and eight commercial firms) on a U.S. trade blacklist, due to Beijing’s treatment of Uighur Muslims and other predominantly Muslim ethnic minorities in China’s Xinjiang province. These developments reflect the continued escalation of sanctions enforcement under the Trump Administration, which as of recent events shows no sign of slowing.

Relatedly, 2019 is likely to be a near record year for OFAC enforcement actions, with settlements reached in 26 enforcement actions that resulted in nearly $1.3 billion in penalties from a cross-section of companies. While past years have seen large settlements focused on financial organisations, 2019 saw actions taken against companies as varied as Apple and e.l.f. Cosmetics, a California-based cosmetics company.

Binning: The six-year-old procedure for Deferred Prosecution Agreements (DPA) which came into force in 2014 continues to attract critical attention. There have so far been six DPAs in England, the first with Standard Bank in 2015, the second against Sarclad Limited, a third with Rolls-Royce, a fourth with Tesco Stores Limited, a fifth with Serco Geografix Limited and the latest one with Guralp Systems Limited.

One of the main points of criticism has been the complete failure to mount a successful prosecution of any individuals after any of the DPAs. The prosecutions of individuals which were initiated in Sarclad, Tesco and Guralp have all failed to secure convictions. Two individuals now await trial in relation to the Sarclad Geografix case.

Other criticism of the DPA regime focuses on there being insufficient incentive for companies to enter a DPA. In particular, the penalty discount is no better than for a guilty plea. There certainly is a forceful argument for caution before a company commits to this route. The deterrent capability of the SFO and its ability to prosecute companies when a DPA is not agreed is open to serious question. More information will emerge about this from the Barclays case when reporting restrictions are lifted later this year. In that case, the SFO case against the bank was dismissed by the trial judge and a later attempt to reinstate the charges failed at the High Court in October 2018.

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

Thukral: The most significant recent case is the very recent approval of a DPA entered into between Airbus and the SFO by the English courts [Judgment of Dame Victoria Sharp P. of 31 January 2020]. The agreement is part of a €3.6bn global settlement with French and US authorities. The judgment makes clear that prosecution of a corporate is perfectly possible notwithstanding the collateral consequences on its employees or the public at large. As the judge explained, “No company is too big to prosecute.”

In addition to the Airbus case, the SFO recently entered into DPAs with Serco Geografix (July 2019) in respect of the accounting of profits for the provision of electronic monitoring services to the Ministry of Justice and Guralp Systems (December 2019) in respect of the payment of bribes and failure to prevent bribery by employees. Corporates and their legal advisers will be examining these cases closely to understand what lessons they can learn in terms of the approach of the enforcement authorities to investigation and prosecution, cross-jurisdictional cooperation, and the evaluation of compliance programmes.

Ruck: In April 2019, the UK Supreme Court granted KBR Inc. leave to appeal against a decision that allowed the SFO to compel certain foreign companies to hand over documents held overseas.

KBR Inc. is appealing the judgment in R (on the application of KBR Inc) v The Director of the Serious Fraud Office (2018) EWHC 2012 (Admin) (KBR v SFO), in which the Administrative Court held that section 2(3) of the Criminal Justice Act 1987 (CJA), which (broadly) gives the SFO power to require a person to produce specified documents in connection with an SFO investigation, has certain extra-territorial effect. The Court held that section 2(3) CJA operates with extra-territorial effect to compel a foreign company to produce documents held outside the jurisdiction where there is a ‘sufficient connection between the company and the jurisdiction’ (even though no such test is included in the statute). The Court also indicated that a section 2(3) notice can be used to compel a UK company to produce documents that are held on a server outside of the jurisdiction.

The decision in KBR v SFO was controversial and generally criticised for seeking to support UK authorities’ assertion of extraterritorial information gathering powers by applying a wholly purposive and contextual interpretation to the legislation granting those powers. The decision has also had an impact beyond SFO investigations because the ‘sufficient connection’ test has been applied to give extraterritorial effect to certain of HMRC’s powers.

The trial of former Barclays executives commenced in January 2019. We saw John Varley acquitted following a submission of no case to answer, the jury discharged and a decision by the Court of Appeal to uphold the acquittal. The start of the retrial of the three remaining individuals began in October 2019 and is ongoing at the time of writing. This all followed the Crown Court’s decision, in May 2018, to dismiss charges against Barclays Plc and Barclays Bank Plc, and an unsuccessful application by the SFO to the High Court seeking reinstatement of those charges. Given the public profile of the case and its recent history, there is little doubt that this case is an extremely important one for the SFO and that the reputational consequences for the SFO of convictions or acquittals will be significant.

““The most significant recent case is the very recent approval of a DPA entered into between Airbus and the SFO by the English courts [Judgment of Dame Victoria Sharp P. of 31 January 2020]. The agreement is part of a €3.6bn global settlement with French and US authorities.”

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

Poston: The U.S. v. Hoskins case¹ is the first FCPA case in which a foreign national was tried to verdict (11/8/19, D.E. 583). On 8 November 2019, a jury convicted Hoskins on 11 counts — six counts of violating the FCPA, three counts of money laundering, and two counts of conspiracy.

Background

In 2012, a grand jury charged Hoskins with violating the FCPA for his alleged involvement in a multimillion dollar bribery and money laundering scheme. Hoskins engaged in a conspiracy to pay bribes to officials in Indonesia in order to win a $118 million contract under which Alstom Power Inc., located in Connecticut, and its partner, Marubeni Corporation, would provide power-related services to citizens of Indonesia.

Agency

Hoskins sought to dismiss the FCPA counts by claiming that as a foreign national who had never visited the United States, he was not subject to liability under the FCPA.

The government alleged that Hoskins was an agent of Alstom Power because he was responsible for “oversight of the hiring of consultants in connection with Alstom’s and Alstom’s subsidiaries’ efforts to obtain contracts with new customers and to retain contracts with existing customers in Asia, including the Tarahan Project in Indonesia.”

The defence focused on the lack of control that Alstom Power had over Hoskins. The defence explained that the senior employee at Alstom Power, in charge of the power-services project, was not Hoskins’ boss and that “no one at the subsidiary could tell [Hoskins] what to do.”

Ultimately, the Second Circuit concluded that the government could seek to hold foreign nationals liable for violations of the FCPA if the foreign national was an agent of a U.S. domestic concern.

Key Takeaways

The FCPA does not define the term agent, so courts have resorted to traditional agency law principles to evaluate whether an individual qualifies as an agent under the FCPA.

In Hoskins, the jury found agency where (a) the agent was a foreign national, (b) was not employed by the same company as the principal, (c) did not have a formal agreement with the principal, (d) was not controlled by the principal at all times, or such control might have been ineffective, and (d) he was not in charge of the bribery strategy. Thus, this theory of agency sets a low bar for future FCPA enforcement actions.


Rucking: For the first time, a foreign national has been convicted of violating the FCPA. The jury convicted Hoskins on 11 counts: six counts of violating the FCPA, three counts of money laundering, and two counts of conspiracy. The jury found that Hoskins was an agent of Alstom Power Inc. for the purpose of violating the FCPA. Hoskins argued that he was not subject to liability under the FCPA because he was a foreign national. However, the court ruled that foreign nationals can be held liable under the FCPA. The case sets a precedent that foreign nationals can be held liable for violations of the FCPA.

Q4. Can you outline the key fraud & white collar crime trends?

Rucking: Most bribery cases investigated by the SFO have been subject to a deferred prosecution agreement (DPA), including Tesco Stores Ltd, Serco Geografix Ltd and Rolls Royce. We have seen little evidence so far of the SFO having a significant appetite to pursue criminal prosecutions of corporates under this legislation.

The first, and only, criminal conviction in relation to the section 7 offence of a corporate failing to prevent bribery was the Sweett Group Plc in December 2015. The CPS prosecution of Rapid Engineering Supplies Limited for failure to prevent bribery was unusual in that it was not brought by the SFO but this case was dropped along with charges against two individuals in December 2019.

Whilst the SFO has shown a willingness to bring criminal prosecutions against individuals, this has resulted in a number of not guilty verdicts. The difficulty with this is that misconduct described within a DPA often refers to misconduct of senior individuals or the “controlling mind” of the corporate who are subsequently acquitted in criminal proceedings. This disjoint must raise questions as to the appropriateness of the DPAs which have been entered into.

We can also expect to see an increased use of Unexplained Wealth Orders (UWO) as introduced by the Criminal Finances Act 2017. We may also potentially see the use of immunity being conferred by the SFO under section 71 of the Serious Organised Crime and Police Act 2005 (SOCPA) and the use of section 73 SOCPA by the SFO to offer suspects a ‘deal’ with an expectation, but no guarantee, that the Court will reduce any sentence. The SFO has made it clear that it is exploring the use of such cooperating witnesses and its current Director, Lisa Osofsky, has expressed her wish to explore the use of such tools.

We may also see the arrival of the long discussed corporate criminal offence of failing to prevent financial or economic crime modelled on section 7 of the Bribery Act.
Q4. Can you outline the key fraud & white collar crime trends?

Poston: I believe the DOJ’s efforts to achieve transparency, when it comes to what it expects from companies if they are to benefit under its Corporate Enforcement Policy, has been one very noticeable white collar trend.

As background, this Corporate Enforcement Policy began as a pilot programme in 2016, and was formally introduced in November 2017. Under this Policy, DOJ will discount fines against companies that self-disclose foreign bribery, remediate the problem, and cooperate fully with the DOJ. Where all three factors are met and there are no aggravating factors, (e.g. managerial involvement, lengthy criminal behaviour) the company will receive a “declination” of prosecution, provided the company surrenders its ill-gotten gains.

The DOJ’s Corporate Enforcement Policy says: (a) a company should tell the DOJ when it is “aware” of evidence outside its possession, and (b) calls for information “on any individuals” who played a substantial part in the “misconduct.”

These clarifications were meant to relieve “tension” with another provision requiring companies to disclose the conduct reasonably soon after learning of a potential violation. It also lifted any potential perception that a company determine there was a “violation” so early on in its internal investigation.

The DOJ understands that a company “may not be in a position to know all relevant facts at the time of a voluntary self-disclosure, especially where only preliminary investigative efforts have been possible.”

In that situation, a company should “make clear that it is making its disclosure based upon a preliminary investigation or assessment of information, but it should nonetheless provide a fulsome disclosure of the relevant facts known to it at that time.”

The head of the DOJ’s Criminal Division has extended this FCPA Corporate Enforcement Policy to other corporate criminal cases handled by Main Justice, a welcome new trend.

Keenan: Some questioned what the future held for FCPA enforcement under the Trump administration. Although resolving investigations commenced prior to Trump taking office, 2019 reported significant enforcement of the FCPA including two settlements (assessed in US enforcement documents) that broke the “Top 5” namely Ericsson (#2 at $1.06 billion) and MTS (#4 at $850 million). The DOJ and SEC prosecuted more than a dozen companies collectively securing penalties of $2.9 billion. It appears that we have not seen an abatement of FCPA cases with the FCPA Tracker recording in excess of one hundred companies disclosing ongoing investigations.

The SEC’s recent enforcement report for FY2019 reported 862 enforcement actions, the highest level since 2016. Through these actions, the SEC obtained judgments and orders totalling more than $1.1 billion in penalties and $3.2 billion in disgorgement. The level of disgorgement and money returned to investors ($1.2 billion) was the highest level for the past five years driven primarily due to the settlement of Ponzi allegations filed against a Florida-based investment company. It is worth noting that the level of penalties levied was among the lowest in the last five years.

On 1 November 2019, the U.S. Supreme Court agreed to consider whether the SEC has the authority to seek disgorgement at all (the Liu Petition). This could have implications not only for the SEC but also other US agencies who routinely seek disgorgement, such as such as the CFTC, FTC, FDA, and CFPB. The majority of the 526 standalone cases concerned investment advisory and investment company issues (36% of cases) as the SEC makes good on its promise to protect Main Street investors. Securities offerings represented 21% of cases with issuer reporting/accounting and auditing representing 17.7% which is comparable to the prior year. Other cases included market manipulation, insider trading, FCPA enforcement and cases against broker dealers.

Junc: A key trend in U.S. corporate enforcement has been increased incentives for companies to voluntarily self-disclose misconduct and to cooperate more fully with government investigations, including by providing information about individual wrongdoers. This continues a trend that began under the Obama administration, and has continued through the Trump Administration with several policy and guidance pronouncements.

In 2016, the Obama administration released the FCPA Corporate Enforcement Policy, which began as a pilot programme and was later extended to become non-binding guidance for even non-FCPA investigations brought by the DOJ’s Criminal Division. In 2019, the DOJ continued to revise the steps necessary to qualify for self-disclosure and cooperation credit, including its most recent pronouncement in November 2019. These recent changes included relaxing the self-disclosure credit requirements so that companies need only disclose “all facts that are relevant to the investigation, even when not specifically asked to,” and removing language that appeared in prior iterations that required the disclosure of relevant facts the company “should be aware of.”

In mid-December 2019, the DOJ also revised and reissued the National Security Division’s policy regarding voluntary disclosures of export control and sanctions violations, which, like the FCPA Corporate Enforcement Policy, details the benefits available to companies that voluntarily disclose a violation, fully cooperate, and timely and appropriately remediate. This guidance covers similar areas such as requiring “disclosure[] of all relevant facts known to it at the time of the disclosure, including as to any individuals substantially involved in or responsible for the misconduct at issue.” As with the FCPA Corporate Enforcement Policy, the updated policy reflects DOJ’s continued emphasis on corporate voluntary self-disclosure, by rewarding cooperating companies with a presumption in favour of a non-prosecution agreement and substantial penalty reductions.

The trend of incentivising corporate cooperation can also be seen outside of DOJ policies. For example, at an April 2019 conference on litigation and enforcement trends, SEC officials noted the importance of corporate cooperation and noted that going forward its orders would include language that emphasized the specific types of cooperation the SEC had deemed significant, in order to encourage and guide future corporate conduct. In addition, 2019 also saw both French and British regulators publish guidance on expectations for cooperation during an investigation. We expect this trend to continue in 2020, both in the U.S. and abroad.

Binning: The decade long boom in international fraud and regulatory litigation arising from the 2008 global financial crash is all but finished. The next big thing has yet to emerge but it is likely to involve cybercrime and data loss as well as tougher regulatory enforcement of professionals. Regulation more widely may be cast aside as populist governments seek growth and promote more laissez faire capitalism. The risk of very large-scale fraud and corruption is as high as it ever was and may be harder to detect as law enforcement technology lags behind the market.

Rebekah J Poston

Ryan D. Junck

Neil Keenan

Peter Binning
Q5. How about compliance and enforcement trends?

Thukral: On the criminal side, we should expect to see government continue to pursue a pro-active approach to enforcement of the criminal law against companies. The recent swathe of concluded and approved DPAs has built up institutional knowledge and experience which means that agencies will now act with increased confidence against corporates.

The position as regards individual criminal responsibility is less clear. While the evidence suggests that the authorities are now using new legislative tools such as Account Freezing Orders, Account Forfeiture Orders and Unexplained Wealth Orders more frequently, it seems that the SFO may be less willing to prosecute individuals where it has obtained a financial penalty by way of a DPA. There may be room in the future for individuals to enter into similar agreements with the authorities and thereby avoid possible criminal conviction. Relatedly, the SFO’s enthusiasm for co-operators in criminal cases appears to continue and we may see an increasing number of “plea agreements” entered into.

On both the criminal and civil side, we will continue to notice the impact of technology and machine learning tools on investigations and disputes such that the key documents and issues will be identified more quickly. This should increase the speed with which disputes are resolved. They will also assist in the development of fraud prevention strategies and a greater awareness of how compliance programmes operate in practice, particularly in riskier jurisdictions.

Ruck: The FCA has recently turned its focus to investigations of senior manager conduct and financial crime, amongst other issues. Given the recent extension of the Senior Managers and Certification Regime in the UK to all FCA and PRA regulated firms, we will inevitably see a trend for the FCA and PRA to seek to hold senior managers to account for any regulatory failings.

Whilst the FCA has undertaken dual track investigations (concurrent criminal and regulatory/civil investigations) previously in relation to market abuse, it has now expanded this approach to areas including anti money laundering system and control issues. This is an attempt by the FCA to encourage firms to engage in this area due to the severity of a potential criminal sanction if they do not.

The FCA has continued to increase the number of investigations it has open, including both those relating to corporates and individuals. The PRA has also increased its enforcement capability over the past 12 months and is seeking to illustrate its teeth to those it regulates.

Poston: (i) FCPA

FCPA enforcement in 2019 was in line with 2018. More than half of the settlements involved companies from over six industries, with life services and natural resources most commonly penalised.

Financial services have only recently been targeted with all seven resolutions happening since 2015:

- BNY Mellon
- Och-Ziff Capital Management
- JPMorgan Chase
- Credit Suisse
- Société Générale
- Legg Mason, and
- Deutsche Bank

(ii) OECD

All these telecom companies received fines between $800 million and $1 billion since 2016.

Over the past several years, there has been an emerging trend of sharing evidence and splitting the financial penalties among prosecuting sovereigns. This was clearly demonstrated in the Odebrecht case in Brazil. In 2016, the DOJ assessed a total penalty against Odebrecht of $2.6 billion. 10% was payable to the U.S., the rest payable to Brazil and Switzerland.

After the resolution, Odebrecht’s ability to pay was reduced by its loss in business. DOJ reduced its share of the criminal penalties down from $260 million to $93 million. Odebrecht then declared bankruptcy. So it remains unclear what the U.S. will receive in its share of penalties from Odebrecht.

(iii) OFAC

In the OFAC sanctions arena, OFAC announced 26 enforcement actions targeting U.S. companies for sanctions violations committed by acquired non-U.S. affiliates or subsidiaries. This netted OFAC nearly $1.3 billion in civil penalties, as well as three additional findings of violations, making 2019 one of the most active enforcement years on record.

Last year, OFAC increased its scrutiny of U.S. private equity sponsors over sanctions violations committed by majority owned or controlled portfolio companies. Even though private equity sponsors generally have limited authority over the day-to-day operations of the companies in which they invest, it appears OFAC sees it differently. Private equity sponsors have equivalent compliance obligations for portfolio companies, as corporate parent companies do for their subsidiaries according to OFAC.

Given the geopolitical instability around the world, there is no reason to believe 2019’s active enforcement trends will not continue into 2020.

Miralis: Recent developments in combating fraud and white collar crime have in-part been driven by the Australian Transaction Reports and Analysis Centre (AUSTRAC). Of particular relevance has been the evolving role of the Fintel Alliance, a partnership of public and private organisations, led by AUSTRAC, intended on sharing intelligence in order to combat and disrupt serious financial crime.

In its 2018-19 report on Fintel, AUSTRAC indicated that across the reporting period six Fintel operations had been conducted relation to the exploitation of government revenue, a further six operations related to complex financial crime, and numerous other operations concerned countering foreign bribery and corruption.

In the 2019-20 Budget, the Australian Government announced new funding of $28.4 million to AUSTRAC over four years to continue and expand Fintel Alliance operations.
Q5. How about compliance and enforcement trends?

Le Cornu: Guernsey, as with all offshore financial centres, has been under pressure from onshore centres in recent years to be more transparent and to reduce the likelihood of being used to facilitate the movement or concealment of the proceeds of crime, including tax evasion. Guernsey has responded by introducing a highly effective regulatory regime, including many of the laws referred to above.

One other recent introduction is the Beneficial Ownership of Legal Persons Law, 2017 (“BOL”) which came into effect on 17 August 2017. The BOL requires details of the beneficial ownership of legal entities to be provided to the Guernsey Registry. That information is not available publicly, but may be accessed under strict protocols by law enforcement agencies and is another example of Guernsey’s commitment to combating financial crime and terrorist financing.

In 2018, the Financial Crime Division of the GFSC conducted 47 on site visits, almost half of which were undertaken in conjunction with the Investment, Fiduciary and Pension Division as part of a thematic review of adherence to the BOL. That review continued into 2019 with the GFSC concluding that there was a widespread commitment in the financial services sector to accurately identify beneficial owners. Some of those firms visited were not fully compliant with the legislation or regulations and were required to follow one of three courses of action: Two firms were referred to the Enforcement Division for further investigation, another two were required to appoint a third party to review their remediation programme, or where more serious breaches were identified conditions were imposed on their license to restrict certain activities (three firms).

Meanwhile, the GFSC’s Enforcement Division reported the number, size and complexity of the cases it was seeing increasing. Seven new cases were referred to the Enforcement Division during 2018, whilst it had 12 cases carried over from 2017. The Enforcement Division’s primary focus is reviewing fiduciary firms to ensure they are compliant with the various laws and regulations imposed on those firms with a high focus on Anti Money Laundering and Countering Terrorist Financing provisions, the protection of investors and the reputation of the island as a major international financial centre. If, during the Enforcement Divisions reviews, instances of financial crime are uncovered, they are referred to the Financial Investigation Unit (see below).

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.

Keenan: The DOJ has continued to require in some instances, as a term of Deferred Prosecution Agreements, the appointment of a compliance monitor. In October 2018, the DOJ issued guidance (the Benzczkowski Memo) with respect to whether a corporate monitor should be appointed. The memo provides specific guidelines for making that determination including: 1) whether the corporation has since bolstered and improved its compliance program and internal controls; and 2) whether improvements to the corporate-compliance program and internal controls have already demonstrated that they prevent similar misconduct in the future.

While an investigation is expensive, time consuming and removes resources from the day to day operations of the business, it is essential that companies undertake a "root cause" analysis of why illegal acts took place, what control weaknesses enabled the conduct to occur undetected, and take timely steps to address such weaknesses and enhance the compliance program. Ideally such efforts should take place as the investigation proceeds and not be deferred until settlement discussions have commenced or are nearing conclusion.

Unfortunately, we see a trend of companies failing to take steps to remediate known issues in a timely manner. As noted in the Benzczkowski Memo, a company must have already demonstrated that the improvements to the compliance program/control environment are operating effectively and this requires both time, and monitoring/testing.
Q6. Which government agencies investigate fraud & white collar crime?

Ruck: The SFO is the main prosecutor with responsibility for enforcing the Bribery Act in England and Wales. The FCA has the power to prosecute the following criminal offences, except in Scotland where the Crown Office retains this responsibility:

- Insider dealing (Part V, Criminal Justice Act 1993)
- Making false or misleading statements, creating false or misleading impressions, and making false or misleading statements or creating a false or misleading impression in relation to specified benchmarks (Part 7, Financial Services Act 2012).

In relation to the civil offences in MAR, the FCA may impose an unlimited financial penalty, prohibit regulated firms or approved persons, make a public statement of the person’s misconduct, apply for an injunction to restrain threatened or continued misconduct or an injunction requiring a person to take steps to remedy misconduct or a freezing order, apply for a restitution order and/or require the payment of compensation to victims.

Poston: A multitude of agencies investigate fraud and white collar crime. In the FCPA world, the DOJ and SEC are the criminal and civil enforcement agencies, respectively, that jointly investigate and prosecute FCPA cases. The bribery and corruption provisions are prosecuted by the DOJ, and the accounting provisions, or books and records and internal controls provisions, are prosecuted by the SEC.

Joint task forces have been the trend over the past years. Counts of FCPA are paired with wire fraud and money laundering. Healthcare fraud is paired with wire fraud, tax evasion and money laundering. Immigration fraud is paired with labour and employment and tax evasion. On these government joint task forces are FBI, HSI, ICE, CBP, DOL, DEA, IRS/CID, Secret Service, Postal Inspectors, FinCEN and CFTC.

Like the DOJ, criminal defence counsel need to build their own joint task forces and include on them attorneys competent in civil and commercial law, immigration, labour and employment law, data privacy, cybercrime, and criminal law.

Miralis: Given the sophistication and complexity of white-collar crime, often various government agencies are involved in various aspects/stages of their investigation. These stages include prevention, detection, investigation and prosecution of offences, and recovery of the proceeds of crime.

A broad overview of the centrally relevant agencies is as follows:

i. The Australian Tax Office (‘ATO’)
   The ATO conducts criminal investigations related to serious and/or complex fraud related to Australia’s taxation and superannuation systems.

ii. The Australian Federal Police (‘AFP’) and other state Police forces
   The AFP has primary responsibility for investigating a range of criminal offences under Commonwealth law, including serious and complex fraud against the Commonwealth.

Further, state Police forces often contain dedicated fraud squads whose roles exclusively cover serious white-collar criminal activity.

iii. The Australian Criminal Intelligence Commission (‘ACIC’)
   The ACIC is Australia’s national criminal intelligence agency, with work priorities that include targeting criminal wealth. The ACIC investigates a vast range of sophisticated and large-scale white-collar criminal activity and closely collaborates with other Australian law enforcement agencies in doing so.

iv. The Australian Transaction Reports and Analysis Centre (‘AUSTRAC’)
   AUSTRAC, Australia’s financial intelligence unit, assists law enforcement and various government agencies in the investigation and prosecution of financial and tax crime.

v. The Australian Prudential Regulation Authority (‘APRA’)
   APRA is the prudential regulator of the Australian financial services industry.

vi. The Australian Securities and Investments Commission (‘ASIC’)
   ASIC enforces financial services and corporation laws.

vii. The Commonwealth Director of Public Prosecutions (‘CDPP’)
   Australia’s independent federal prosecution agency, the CDPP, prosecutes offences against Commonwealth laws, including fraud and white-collar cases.

Le Cornu: The principal government agency tasked with investigating fraud and white collar crime in Guernsey is the Financial Investigation Unit (“FIU”), a division of the Guernsey Border Agency (“GBA”). The FIU is comprised of three teams, the Financial Intelligence Service (“FIS”), which is jointly staffed by Guernsey Police and GBA staff, the Financial Criminal Team (“FCT”) and the Civil Forfeiture Team (“CFT”).

The FIU’s objective is to prevent and combat financial and economic crime to maintain and uphold Guernsey’s integrity as a major international finance centre. The GBA focuses its attention in complying with FATF recommendations, the requirements of the IMF and other international regulatory and supervisory bodies.

The FIS is the body which is charged with receiving and acting on all STRs. The FIS analyses the STRs and where appropriate disseminates information to other law enforcement bodies and agencies internationally. This information is usually related to the proceeds of crime either domestically or internationally. In some instances, the FIS may take action to seize assets which are the proceeds of crime that are located within the Bailiwick.

Binning: The Serious Fraud Office mainly and the police advised by the Crown Prosecution Service.

Poston: Further, state Police forces often contain dedicated fraud squads whose roles exclusively cover serious white-collar criminal activity.

Ruck: The SFO is the main prosecutor with responsibility for enforcing the Bribery Act in England and Wales. The FCA has the power to prosecute the following criminal offences, except in Scotland where the Crown Office retains this responsibility:

- Insider dealing (Part V, Criminal Justice Act 1993)
- Making false or misleading statements, creating false or misleading impressions, and making false or misleading statements or creating a false or misleading impression in relation to specified benchmarks (Part 7, Financial Services Act 2012).

In relation to the civil offences in MAR, the FCA may impose an unlimited financial penalty, prohibit regulated firms or approved persons, make a public statement of the person’s misconduct, apply for an injunction to restrain threatened or continued misconduct or an injunction requiring a person to take steps to remedy misconduct or a freezing order, apply for a restitution order and/or require the payment of compensation to victims.
Q7. How are cross border investigations conducted?

Thukral: Where there is a U.S.-aspect to an investigation or prosecution, it is generally the U.S. authorities which take the lead in such cases with their foreign counterparts assisting where appropriate or necessary. However, as the Director Lisa Osofsky has made clear in a series of recent pronouncements, the SFO is determined to increase its cross border cooperation with foreign agencies and enforcement authorities in Europe and beyond.

The recent Airbus judgment is an illuminating case study into the cooperation between U.S., French and UK authorities into a realistic budget in order to cover the scope of work you need to accomplish for the client. A global team’s members should be able to address these issues in order to enable them to operate efficiently within agencies over a sustained period and suggests that this will continue going forward.

Similarly, there have been a series of recent legislative developments which indicate further international cooperation including the Crime (Overseas Production Orders) Act 2019 and the U.S.-UK Bilateral Data Access Agreement in respect of obtaining electronic data directly from an overseas service provider. This will reduce the need for Mutual Legal Assistance Treaty requests and should ensure that enforcement agencies obtain access to information quickly where the applicable conditions are satisfied.

Poston: Internal cross border investigations are conducted with planning. First, you should define the scope of your investigation, which will need to be adjusted as you proceed depending on your findings. Once you know which jurisdictions are involved, it will be essential to the investigation to assemble a global team comprised of local legal counsel schooled in the areas of inquiry. You will need to assess what language capabilities are required on your team, according to what language the documents will be in and what language your witnesses speak. For example, in China, do you need to speak Mandarin or Cantonese?

You must evaluate the restrictions placed upon you regarding evidence gathering and the transport of that evidence out of and between the countries where you will be working; what visas are required to travel and work there; how you obtain legal access to employees (e.g. workers’ unions and their roles); is there government monitoring of phone calls in the country; and what are the security levels in the country?

When evaluating your data privacy issues, you will need to find out where the company’s servers are located. Have the employees already executed consent forms providing permission to search their computers? Do the laws of that country address legal privileges and how expansive are they? Legal privilege varies by country, so who is covered and what communications are protected is critical to assess up front. All these and more issues need to be anticipated and addressed before you begin.

Are your interview staff trained in conducting interviews if they come from a non-litigation jurisdiction? If not, you may need to transport your U.S. personnel to do the interviews. A global team’s members should be able to address these issues in order to enable them to operate efficiently within a realistic budget in order to cover the scope of work you need to accomplish for the client.

Keenan: Cross border investigations are often gruelling, time-consuming, expensive, and difficult depending on the unique circumstances. Investigations are only getting more complex for companies and their legal and forensic advisors, primarily due to the number of enforcement agencies that might have an interest, and the increasing number of laws and regulations around how data can be obtained, processed and reviewed.

It is critical that companies collect information and data whilst observing a host of data laws and regulations: data privacy, blocking statutes, state secrecy acts, and localisation requirements. Falling foul could result in greater issues, for a company and individuals, than the initial area under investigation. Data specialists can find creative ways of obtaining necessary records and preserving and processing such data in a way that minimises privacy concerns. Examples include maintaining records in a secure environment housed at a company’s premises, creating multiple data-rooms for the sharing of information based on the geography of those reviewing the information, removing metadata attached to files and redacting certain personal information. This does, however, add costs and require incremental time to resolve an investigation.

Another essential component is understanding what potential jurisdictions and agencies may have an interest. Enforcement agencies around the world have varying expectations with respect to how investigations are performed and this must be considered prior to proceeding with investigation steps, for example, witness interviews. In addition, company’s may wish to exert privilege over work performed and product produced, but will have to address differing interpretations on what constitutes and is covered by legal privilege in different countries.

In order for cross border investigations to be effective, you also need to take into consideration business practices and the culture of the country in which you are investigating. For example, many international markets will use ephemeral messaging apps for business communications (e.g. WeChat in China). The use of such messaging apps pose a significant compliance issue for companies in terms of a policy on their use and how, if at all possible, the company can access and preserve such business records. It also creates challenges for investigation teams to access potentially relevant corporate records. This issue has been recognised by the DOJ who have released a policy on this issue, the latest refinement released in March 2019.

"The recent Airbus judgment is an illuminating case study into the cooperation between U.S., French and UK authorities into bribery across several different jurisdictions."

- Ravinder Thukral -
Q7. How are cross border investigations conducted?

Junck: One key to conducting cross border investigations is the collection of information from other jurisdictions outside the U.S. In order to effectively pursue a cross border investigation, there are a few different methods by which U.S. authorities can obtain the information they require from other countries' regulators.

For instance, the DOJ can obtain foreign evidence and cooperation through the use of Mutual Legal Assistance Treaties (MLATs) with foreign criminal authorities. The SEC’s Office of International Affairs has the ability to work through several international mechanisms for information requests, including the International Organization of Securities Commissions and the Multilateral Memoranda of Understanding, which facilitate the exchange of information between the SEC and other securities regulators.

Even with these mechanisms, U.S. regulators are heavily reliant on companies cooperating with the investigation and finding creative ways to voluntarily turn over documents in response to these requests. Other challenges to collecting information in a cross border investigation include banking secrecy laws, differences in disclosure and data privacy rules (notably the GDPR), blocking statutes, and in some cases, an outright refusal by other countries to comply with such information requests.

In an attempt to alleviate some of these issues, the U.K. and the U.S. recently introduced a new process to facilitate access to electronic data stored by technology companies overseas for criminal investigations and prosecutions, enabling law enforcement authorities to bypass the often cumbersome and inefficient process of obtaining such data through foreign judicial assistance requests. In 2018, the U.S. passed the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), which allows the U.S. government to enter into agreements with other countries that will require communications-service providers subject to U.S. jurisdiction to respond to those countries' requests for data.

Falling in step with the U.S., in 2019 the UK passed the Crime (Overseas Production Orders) Act (the COPO Act), which reflects many of the same principles and potentially goes further by empowering enforcement agencies to compel disclosure from any individual or company operating or based abroad, provided that the UK has a designated international cooperation agreement with the country where the production order will be served. In October 2019, the two governments agreed on a cooperation agreement by signing the UK-U.S. Bilateral Data Access Agreement. Once ratified, it will be the first agreement applicable under the CLOUD Act and the COPA Act.

Binning: Increasingly cross border investigations are being managed closely by collaborating law enforcement officers who know each other and who can work effectively together with more sophisticated methods and tools. As previously mentioned, there are now new powers to obtain documents from foreign servers. There is much more collaboration now than there used to be in global corruption and fraud cases as shown by the introduction in France and other countries of non-criminal conviction disposals like the CPA.

Q8. Can you outline the best practice for corporate governance and internal control considerations?

Thukral: Best practice is informed by being profoundly aware of a corporate’s potential vulnerabilities, the latest guidance and decisions from relevant jurisdictions and the importance of ongoing monitoring and review. The publication by the SFO of its “Evaluating a Compliance Programme” document is a good indication of some of the relevant considerations but it is by no means comprehensive. Best practice requires corporates and practitioners to engage with standards that are relevant to the industry and sector in which they operate. They must also take into account issues around doing business in particular jurisdictions and understand how to craft best practice standards which are culturally and geographically appropriate.

Staff training is a key issue where corporates can continue to improve governance and control. Members of staff are the customer facing part of the business and, if they well trained, they can quickly detect and address fraud and possible criminality at an early stage.

Ruck: Best practice includes, but is not limited to, the following:

- Robust governance arrangements including:
  - A clear organisational structure with well-defined, transparent and consistent lines of responsibility
  - Effective processes to identify, manage, monitor and report the risks the corporate is or might be exposed to
  - Defined individuals who are responsible and accountable for key areas including risk, compliance, AML/financial crime, supervision of outsourcing and remuneration oversight

- Sound internal control mechanisms including:
  - Appropriate administrative and accounting procedures
  - Effective control and safeguard arrangements for information processing systems
  - Client due diligence measures, ongoing monitoring and internal policies and procedures which are appropriate in light of the financial crime risks to the corporate, including bribery, fraud and money laundering
  - Adequate procedures to prevent bribery which would provide the corporate with a defence to the corporate failure to prevent offence in section 7 of the Bribery Act 2010

- Poston: Good corporate governance incorporates internal controls into its overall compliance programme. One cannot go wrong in following the U.S. DOJ’s Corporate Compliance Program guidance. While each company’s risk profile is different, as are the solutions devised to reduce such risks, these basic questions can be asked when evaluating whether a company’s best practices for corporate governance are in place.

  i. Is the company’s compliance programme well designed?
     - Risk assessment
     - Policies and procedures
     - Training and communication
     - Confidential reporting structure and investigative process
     - Third party management
     - Mergers and acquisitions
  
  ii. Is the company’s compliance programme being implemented effectively?
     - Commitment by senior and middle management
     - Autonomy and resources
     - Incentives and disciplinary measures

Thukral: Best practice is informed by being profoundly aware of a corporate’s potential vulnerabilities, the latest guidance and decisions from relevant jurisdictions and the importance of ongoing monitoring and review. The publication by the SFO of its “Evaluating a Compliance Programme” document is a good indication of some of the relevant considerations but it is by no means comprehensive. Best practice requires corporates and practitioners to engage with standards that are relevant to the industry and sector in which they operate. They must also take into account issues around doing business in particular jurisdictions and understand how to craft best practice standards which are culturally and geographically appropriate.

Staff training is a key issue where corporates can continue to improve governance and control. Members of staff are the customer facing part of the business and, if they well trained, they can quickly detect and address fraud and possible criminality at an early stage.

Ruck: Best practice includes, but is not limited to, the following:

- Robust governance arrangements including:
  - A clear organisational structure with well-defined, transparent and consistent lines of responsibility
  - Effective processes to identify, manage, monitor and report the risks the corporate is or might be exposed to
  - Defined individuals who are responsible and accountable for key areas including risk, compliance, AML/financial crime, supervision of outsourcing and remuneration oversight

- Sound internal control mechanisms including:
  - Appropriate administrative and accounting procedures
  - Effective control and safeguard arrangements for information processing systems
  - Client due diligence measures, ongoing monitoring and internal policies and procedures which are appropriate in light of the financial crime risks to the corporate, including bribery, fraud and money laundering
  - Adequate procedures to prevent bribery which would provide the corporate with a defence to the corporate failure to prevent offence in section 7 of the Bribery Act 2010

Poston: Good corporate governance incorporates internal controls into its overall compliance programme. One cannot go wrong in following the U.S. DOJ’s Corporate Compliance Program guidance. While each company’s risk profile is different, as are the solutions devised to reduce such risks, these basic questions can be asked when evaluating whether a company’s best practices for corporate governance are in place.

  i. Is the company’s compliance programme well designed?
     - Risk assessment
     - Policies and procedures
     - Training and communication
     - Confidential reporting structure and investigative process
     - Third party management
     - Mergers and acquisitions
  
  ii. Is the company’s compliance programme being implemented effectively?
     - Commitment by senior and middle management
     - Autonomy and resources
     - Incentives and disciplinary measures
Q8. Can you outline the best practice for corporate governance and internal control considerations?

Keenan: In April 2019, the Criminal Division of the US Department of Justice (DOJ) released a guidance document – “The Evaluation of Corporate Compliance Programs” – for white-collar prosecutors on the evaluation of corporate compliance programmes.

Part I of the document discusses various hallmarks of a well-designed compliance programme relating to risk assessment, company policies and procedures, training and communications, confidential reporting structure and investigation process, third-party management, and mergers and acquisitions.

Part II details features of effective implementation of a compliance programme, including commitment by senior and middle management, autonomy and resources, and incentives and disciplinary measures.

Finally, Part III discusses metrics of whether a compliance programme is in fact operating effectively, exploring a programme’s capacity for continuous improvement, periodic testing, and review, investigation of misconduct, and analysis and remediation of underlying misconduct.

While all aspects are obviously important, two areas deserve increased focus: third party management and periodic testing. Business partners come with considerable fraud risk, such as accounting fraud, corruption, export controls/sanctions and cyber breaches – to name but a few.

Junct: There are a few best practices that a company should keep in mind in terms of corporate governance and internal controls:

- Identify the potential risks the company faces based on its particular industry, activities, and any regulatory regimes to which it is subject.
- Once such issues are identified, analyse which risks are the particularly higher risk areas of the company’s business.
  - This determination may be guided by the jurisdictions in which the company operates or has supply chains, how funds and financial transactions are processed in the company, etc.
  - Structure and adequately staff an internal team to monitor compliance, execute investigations, and perform regular audits of the company’s compliance with its policies and applicable law (particularly for the higher risk areas in the company’s business).
  - This team should integrate and communicate regularly with legal, internal audit, and any other compliance functions.
  - This team should also regularly review the company’s compliance policies, and ensure that the policies are updated with any changes to relevant legislation or guidance provided by regulators.
- Establish an internal reporting mechanism between the team responsible for monitoring and effecting compliance and the management of the company.
  - This reporting mechanism should include both regular, routine reporting (such as annual reviews, presentations to the board on the results of internal audits and internal and/or external investigations), as well as internal reporting requirements that would apply in the context of an investigation (whether internal or external).

Companies need to assess third party risks through a variety of lenses with coordination across departments (e.g., procurement, legal, compliance, IT). With numerous business partners utilised by large international businesses this is a challenging task, but one that cannot be overlooked. This runs throughout the procure-to-pay cycle from on-boarding due diligence through the review of transactional documentation, and subsequent post payment monitoring.

One area of particular challenge is the ongoing monitoring of third parties post contract. Deploying data analytics and dedicated monitoring techniques to assess and respond to changes in the risk profile and business activities, are key to helping companies achieve this.

It is critical to have employees identify and raise the alarm early when fraud is suspected. A good barometer of a compliance programme is the willingness of employees to speak up quickly when they have concerns of potential wrongdoing. Ideally, this should be through line managers and direct reports, as opposed to whistleblower ‘hotlines’. While they have their place, robust programmes not only set the tone at the top but also conduct in the middle. Educating middle management on how to instil the confidence that an employee can speak up without any attribution, blame or repercussions, can identify potential fraud before it becomes more widespread and costly.
Q9. What steps should a company take upon discovering fraud?

Thukral: Upon discovering fraud, it is crucial that a corporate should understand, as far as possible, the factual basis and scale of the allegation. It may need to move rapidly to secure property and documents with the assistance of its external advisers. It should do so by selecting a group of people who are not involved in any aspect of the fraud and who will be responsible for directing the internal and external response. The initial stages of a fraud and a corporate's response to it are crucial to how that fraud is resolved through investigation or litigation. Mistakes that are made in the early stages can create problems which may take many years to resolve fully. If an internal investigation is warranted, there should be support from senior management and relevant staff. A corporate should also consider its self-reporting obligations, issues around legal privilege and how any fraud may affect its contractual obligations towards external third parties.

Ruck: In addition to taking practical steps such as securing potential evidence many corporates who discover evidence of potential serious fraud, bribery or corruption often face a dilemma as to whether they self-report and cooperate with the SFO or not. The Bribery Act 2010, Criminal Finances Act 2017 and the introduction of DPPs have made this decision even harder. The SFO’s recent Corporate Co-operation Guidance published in August 2019 encourages such cooperation and confirms that cooperation will be taken into consideration as a public interest factor against prosecution of a corporate and, potentially, in favour of a DPP.

Whilst this guidance gives some practical steps corporates should take in relation to how information should be provided to the SFO, it is more controversial in relation to the subject of interviewing witnesses and the notes of those interviews. The guidance states that to avoid prejudicing any SFO investigation, the corporate will need to consult with the SFO prior to conducting any such interviews with witnesses or suspects and taking personnel/HR actions or any other overt action.

On a potentially more controversial note the guidance notes that refusing to waive privilege over interview notes may undermine a request for a DPA but will not be ‘punished’ by the SFO. Similarly it requires that where a corporate claims privilege over documents, the corporate must provide a certification by independent counsel that material is privileged.

This trend of seeking to encourage waiver of privilege has also been followed by the FCA with various suggestions by them in correspondence with regulated firms that they may wish to consider waivering privilege. Similarly, the FCA has more recently implemented the process of appointing an internal reviewer, independent of an investigation team, to review any materials identified as privileged during the investigation.

The SFO guidance has left corporates with a lack of clarity on to what extent any internal investigation should be conducted prior to any disclosure to the SFO of potential wrongdoing. Whilst there will need to be some amount of review it remains unclear as to the extent of this. Corporates will need to balance the need to avoid delay in reporting to the SFO to ensure any credit for cooperation is not potentially lost with the need to check whether allegations have any foundation.

The latter may often require initial interviews to obtain further context or background but the SFO guidance suggests such interviews cannot be undertaken prior to a self-report to the SFO.

Le Cornu: The approach taken by companies when they suspect a fraud has been committed can vary greatly. Unless there is clear and irrefutable evidence that a fraud has been committed some firms may prefer to engage a forensic accounting firm to undertake an analysis of the suspect transaction(s), conduct specialist IT forensic analysis of systems and the suspect employee(s) computer (often done out of office hours so as not to alert the employee that they are being investigated), or even to image the suspects mobile phone (where legally allowed) to identify communication with accomplices or other parties.

We had one client who suspected fraud and we were asked to review the accounts and records. The conclusion in that case was that the financial controller of the business was fundamentally out of his depth and had, over a number of years, tried to cover up basic bookkeeping errors. A total lack of basic accounting reconciliations kept the issue out of sight until someone noticed that the cash at bank in the balance sheet did not reconcile to the bank statement by a material amount.

Once armed with evidence of fraud, the firm may elect to report the offence to the police for their investigation and have the person formally charged. In some instances, companies may elect to keep the offence under wraps, due to reputational issues and adverse publicity. This is more likely to be the case where the amount involved is relatively small and a large percentage of the misappropriated funds may be recoverable with the assistance of the perpetrator. In larger cases, particularly in the finance sector, it is more common that the police are brought in at an early stage and charges are ultimately laid.

Poston: Whether fraud is discovered from a whistleblower, through a hotline, or otherwise, the steps are pretty much the same:
• Investigate
• Evaluate and analyse the misconduct
• Remediate the underlying misconduct
• Consider voluntary disclosure to appropriate authorities
• Cooperate if there is voluntary disclosure
• Re-educate and retrain where appropriate
• Continue to monitor and periodically audit compliance

Miralis: Regardless of whether the company is the victim of the fraud or whether it originates internally (i.e. perpetrated by an employee, agent, or associate of the company), companies should take the following swift action in response to a discovery of fraud:
• Stop the occurrence of the fraud
• Preserve relevant evidence
• Seek appropriate legal advice
• Report the matter to law enforcement authorities

However, in relation to instances where the fraud is perpetrated by an employee, agent, or associate of the company, the company should also be mindful of its own potential criminal liability for the offending if swift and appropriate action is not taken.

In addition, in New South Wales a company would be required to report an internally originating fraud to police or risk being prosecuted itself for the offence of concealing a serious indictable offence.

Ravinder Thukral
Michael Ruck
Rebekah J. Poston
Dennis Miralis
Timothy Le Cornu
Q9. What steps should a company should take upon discovering fraud?

Keenan: Companies with more developed compliance programs have likely deployed an Investigation Policy prior to any allegations of misconduct surfacing. While each investigation is fact specific, creating a framework to evaluate and resolve alleged misconduct is important in ensuring that important initial steps are followed thereby maintaining the integrity of the investigation.

Important steps at the outset of an investigation include an appropriate communication channel, assigning overall responsibility (often based on who is allegedly involved or knowledgeable of the misconduct), preservation of relevant data and sources of information, and the evaluation of data governance considerations.

It is also essential to have means of conducting an early discrete assessment to evaluate the potential legitimacy of an allegation as this assists companies in framing the issue and identifying the potential scope and expertise necessary to perform the investigation. This can involve initial steps such as: data analytics of transactions, contracts, projects etc., review of financial information and supporting records, and a discrete review of emails if systems permit.

Such procedures should be overseen by experienced individuals as it requires a fine balance of uncovering sufficient information to make an informed decision, while also maintaining the integrity of the investigation if one is deemed necessary. As facts start to emerge, the company can assess an appropriate scope, and consider if external legal and forensic specialists are needed to fully investigate the allegations raised.

The next item to consider is who will conduct the investigation, and how they will report to management on their progress (i.e., whether it is the legal, compliance, or internal audit team that will sit at the helm of the investigation). Part of this consideration will include whether to create an ad hoc group, such as an audit committee or a special committee, to oversee the investigation.

Additionally, whether to include external counsel should be considered at this stage, and if so, how. As soon as the team conducting the investigation has been determined, steps should be taken to ensure that potentially relevant documents are preserved. Key custodians and the locations of documents should be identified, preservation notifications should be issued, and electronic means of preserving and preventing destruction of data should be taken, if necessary.

These steps will ensure that the company complies with any duties to preserve materials that may have been triggered upon suspicion of misconduct, and that the investigation will be viewed by any outside parties as credible and comprehensive (e.g., enforcement agencies).

Having completed these preliminary steps, a work plan should be drafted outlining the key goals of the investigation, the steps to achieve such goals, the roles and responsibilities of those involved (including external counsel, local counsel, and consultants, if needed), the anticipated timeline for the investigation's completion, and an estimated budget.

Finally, the company should ensure, as quickly as practicably, that any conduct that is either alleged to be (or has been identified as) problematic is halted and remediation steps, such as disciplining employees and revising procedures, are considered and implemented without delay.

Taking such steps at the outset of the investigation will allow the company to better position itself to later demonstrate to the government that the company was fully responsive to the allegations of wrongdoing and deserves full cooperation credit (even in cases where regulators may not initially be involved).

Binning: A company should take care to ensure that it can take prompt legal advice with the benefit of legal privilege protection. A thorough assessment should be made of the fraud discovered and the scale of the perceived problem. Particular attention should be paid to any evidence of third-party loss and a strategy developed to deal with that and to avoid, if possible, damaging litigation instituted by the third parties.

A proportionate approach should be taken in line, ideally, with the company’s existing internal policy for dealing with fraud. A decision about reporting the matter to any outside authority should receive very careful attention and all options should be fully risk assessed taking full account of a company’s due process rights.

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

Binning: Extraordinary though it may seem, it is still too early to tell. Yes, there will be more complex extradition and there will be problems with European co-operation in all aspects of law enforcement and border control. There will be big opportunities for organised criminals and it may take many years to tackle the problem and bring wrongdoers to justice.

Ruck: Whilst Brexit may at first glance create challenges such as the potential loss of the European Arrest Warrant and access to EU shared crime agency databases, any cooperation agreements between the UK and EU law enforcement agencies which are lost will likely be quickly re-established through new legislation, multi-lateral agreements or the practical assistance the UK already gives and receives from non-EU countries. It would be extremely controversial should the mutual benefit to all parties of the fight against fraud and white collar crime not be recognised or cooperation be lost.

“This will be big opportunities for organised criminals and it may take many years to tackle the problem and bring wrongdoers to justice.”

- Peter Binning -