Jeremy Scott-Mackenzie is the Regional Commercial Institutions Manager – Financial Lines, at AIG Australia. He is a leading authority in his field and is responsible for the strategic development of AIG’s Commercial Crime and Directors & Officers Liability insurance portfolio across Australasia, having been with AIG for over 10 years in a variety of roles across the Asia Pacific region. He is a member of the Australian Institute of Company Directors and the National President of the Australian Professional Indemnity Group, Inc.

Neill is a highly experienced fraud and regulatory lawyer who is able to advise clients on the interface between business and regulatory practice and the criminal law. He has particular expertise in advising and representing individuals, corporate clients, professional firms and financial organisations in areas such as market abuse and insider dealing, corruption, money laundering, cartels and price fixing, extradition, bribery and criminal/regulatory compliance.

He has advised on high profile investigations and proceedings brought by the Financial Services Authority (“FSA”), Serious Fraud Office, Revenue & Customs Prosecution Office, the Crown Prosecution Service, Department for Business Enterprise & Regulatory Reform and the Office of Fair Trading. He has advised individuals who have become the subject of a disciplinary investigation in their professional capacity.

Neill has been instructed on some of the largest UK fraud investigations. These include the SFO investigation into benchmark rigging, investigation into financial irregularities at a large supermarket chain and as well as various corruption investigations for major corporates. As well as being involved in a whole host of complex investigations by other bodies such as the CPS, HMRC, FCA and the CMA.

Neill also offers compliance advice and the development of bespoke compliance programmes in areas such as bribery and corruption and money laundering. In particular, he has advised clients on the US Foreign Corrupt Practices Act and its implications for their business, particularly where they perform public contracts in “red flag” countries like Nigeria and China. He is also advising on the impact of the UK Bribery Act and is helping clients devise suitable anti-corruption programmes. He has also provided extensive training on the subject world-wide. He also sits on the CBI Anti-Bribery Working Committee.

Ellen Zimiles is a Managing Director and Head of the firm’s Global Investigations and Compliance practice as well as Leader of the Financial Risk & Compliance Segment. She has more than 25 years of litigation and investigation experience. As an assistant United States attorney in the Southern District of New York for more than 10 years, Ellen served in the civil and criminal divisions and was chief of the forfeiture unit for more than six years. She was responsible for many high-profile money laundering, fraud and forfeiture cases.

Ellen Zimiles is a leading authority on FATCA and has co-authored several articles on FATCA in the past year, most recently a FATCA Highlights brief summarizing the recent FATCA Proposed Regulations. She has been quoted on FATCA in several publications, including American Banker.

Ellen’s experience also includes the development of anti-money laundering programs, corporate governance, regulatory and corporate compliance, fraud control, and public corruption matters. She has worked with a multitude of financial institutions preparing for regulatory exams, developing remediation programs and assisting organizations as a regulatory liaison.

Neill Blundell - Eversheds
T: +44 (0) 20 7919 4533
E: neillblundell@eversheds.com
W: www.eversheds.com

Ellen Zimiles - Navigant Consulting
T: +1 646 227 4612
E: ellen.zimiles@navigant.com
W: www.navigant.com

Jeremy Scott-Mackenzie - AIG
T: +61 2 9240 1712
E: jeremy.scott-mackenzie@aig.com
W: www.aig.com
Kevin Dooley Kent - Conrad O’Brien PC
T: +1 215 523 8306
E: kkent@conradobrien.com
W: www.conradobrien.com

Kevin Kent represents corporations and professionals in a broad range of complex commercial litigation focusing on class actions, civil fraud, director and officer liability, legal malpractice, fiduciary, trademark, copyright, and employment litigation. A substantial portion of Kevin’s practice involves internal investigations and white collar criminal defense, including grand jury investigations overseen by U.S. Attorneys’ offices, and the defense of clients in parallel civil litigations.

Robert N. Sikellis - Siemens AG
E: robert.sikellis@siemens.com
W: www.siemens.com

Robert N. Sikellis assumed his current position as Chief Counsel Compliance for Siemens AG on October 1, 2014, based in Munich, Germany. In this capacity, Mr. Sikellis leads the Compliance Governance Organization for the legal Compliance management, Compliance policies, internal investigations, disciplinary sanctions and remediation and Compliance in Mergers and Acquisitions.

Prior to assuming his current position, Mr. Sikellis held a number of other leadership roles within Siemens, including most recently Senior Vice President & General Counsel of Siemens North East Asia and Siemens Ltd., China. In this function, he was responsible for all legal and compliance in the region and was a member of the Leadership Team in the region. Before China, Mr. Sikellis was General Counsel, Regional Compliance Officer and Member of the Board of Directors for Siemens AE (Greece), based in Athens, Greece, as well as at Siemens AG Headquarters in Munich, Germany, where he was assigned to the Legal & Compliance organization.

Prior to joining Siemens in 2008, Mr. Sikellis was Associate General Counsel and Managing Director for a large U.S.-based consulting firm. He remained in this position for over 10 years, handling the full range of commercial and corporate issues facing a large consulting corporation.

Previously, Mr. Sikellis was the Chief of the Attorney General’s Special Criminal Investigations Division based in Massachusetts (USA). As Chief Director of the Special Criminal Investigations Division, he oversaw and supervised all investigations and prosecutions for the Division, including the High Technology Crime, Narcotics, Organized Crime, Arson and Asset Forfeiture Units. Prior to being appointed Chief Director, Mr. Sikellis was an Assistant Attorney General assigned to the Attorney General’s Special Criminal Investigations Division, where he prosecuted hundreds of criminal cases, ranging from complex white collar to organized crime to money laundering offenses.

Jason Mansell - QEB Hollis Whiteman
T: +44 (0) 207 933 8855
E: jason.mansell@qebhw.co.uk
W: www.qebhw.co.uk

Jason provides strategic advice and representation to firms and individuals facing investigation and potential criminal prosecution by the SFO and prosecution and/or disciplinary action by FCA and other regulatory bodies including the FRC. A formidable advocate, Jason has acted for firms and individuals in connection with over 85 FCA/FSA regulatory investigations and associated proceedings. He also acts for individuals and corporates in some of the more high profile and complex criminal prosecutions. Many of his cases result in no formal public action. Jason is currently acting for two individuals in connection with investigations by the SFO and FCA in relation to the alleged manipulation of LIBOR, a PLC Bank and an individual in connection with FOREX as well as numerous FCA investigations and proceedings for market abuse and breaches of FCA Rules and Principles. Past cases include FCA-v-Koutsogiannis (LIBOR investigation with no action taken), FCA-v-Moorhouse Group, FCA-v-Capital Alternatives Limited (Court of Appeal), FCA-v-X Plc (listing rules investigation with no action taken). He also recently persuaded the RDC not to issue a Decision Notice against a CEO facing prohibition. Previous criminal instructions include R-v-Whelan (market manipulation), R-v-Norton Healthcare (price fixing) and Operation Tabernula (insider dealing). Jason also advises firms on compliance issues under anti-money laundering and anti-bribery legislation.

K R J
Shula de Jersey is a Principal Lawyer in the business crime department at Slater and Gordon in London.

She is an expert in all areas of white-collar crime including high profile fraud, money laundering and corruption and has represented clients in all areas of criminal law including serious crime. She specialises in representing individuals in complex and serious fraud proceedings, health and safety and corporate manslaughter cases and has handled a number of Serious Fraud Office (SFO) investigations. Shula has had articles published in The Lawyer, Legal Week, In-House Lawyer and Telegraph Online and is a consultant editor for Lloyds Law Reports: Financial Crime.

Gary DiBianco represents corporations and their officers, directors and employees in criminal and civil investigations, regulatory matters and complex cross-border proceedings. He has extensive experience defending government inquiries and conducting internal investigations in anti-corruption, fraud, securities and related matters.

Mr. DiBianco has been involved in a number of significant matters representing U.S. and international entities in a variety of industries and business sectors, including, pharmaceuticals and life sciences, oil, gas and mining, financial services, manufacturing and professional services. His experience under the U.S. Foreign Corrupt Practices Act, U.K. Bribery Act and related laws includes global investigations, responses to multinational governmental inquiries and due diligence in connection with corporate transactions.

James Ratley, CFE, serves as President and CEO of the Association of Certified Fraud Examiners, where he works to promote the ACFE to the public and other professional organizations. He also continues to assist in the development of anti-fraud products and services to meet the needs of ACFE’s members, and teaches regularly at workshops and conferences on a variety of fraud-related subjects. Mr. Ratley was selected as one of Security magazine’s Most Influential Security Executives for 2010. This honor is bestowed each year to the top security executives who positively impact the security industry, their organizations, their colleagues and their peers.

Sabine Stetter - Stetter Rechtsanwälte
T: +49 89 13 92 791-0
E: s.stetter@stetterlegal.com
W: www.stetterlegal.com

- 2010 Establishment of Stetter Rechtsanwälte, in Munich.
Set up and managed the department for Commercial Criminal and Regulatory Offence Law.

- 2004 - 2006 Attorney at Leisner Lawyers, Munich. Set up an independent commercial criminal and regulatory offence law practice (including business organizations).
- 2000 - 2003 Active in criminal legal appeal proceedings in front of the Federal Court of Justice with Prof. Dr. Gunter Widmaier with focus on commercial and tax criminal law.

Education
- Ernst-Moritz-Arndt University Greifswald, Doctorate (Dr. jur.) 2006
- District Court Munich I, Second State Examination 2000
- Ludwig-Maximilian University Munich, First State Examination 1998
- London School of Economics
- University of Regensburg

James D. Ratley, CFE, serves as President and CEO of the Association of Certified Fraud Examiners, where he works to promote the ACFE to the public and other professional organizations. He also continues to assist in the development of anti-fraud products and services to meet the needs of ACFE’s members, and teaches regularly at workshops and conferences on a variety of fraud-related subjects. Mr. Ratley was selected as one of Security magazine’s Most Influential Security Executives for 2010. This honor is bestowed each year to the top security executives who positively impact the security industry, their organizations, their colleagues and their peers.
Fraud & White Collar Crime 2016

In our Fraud & White Collar Crime 2016 Roundtable we spoke with 10 experts from around the world. We discover which jurisdiction is experiencing increased levels of sophisticated white collar crime and where technology is shaping the landscape. Other highlighted topics include: cybersecurity, whistleblowing, data and analytics in risk management and court experts and expert witnesses. Featured countries are: United Kingdom, USA, Germany and Australia.

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

Mackenzie: Whilst cyber-crime, such as the theft of personal data, is badly under-reported across Asia Pacific, there is slow legislative movement to address how companies handle these incidents.

As an example, the Australian government has just issued an exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015. This would require notification to the regulator and potentially affected individuals where there has been a more serious data breach. In many cyber fraud incidences, these are not only the loss of corporate assets, but customer or employee data is often compromised, and so we expect that not only will we see an increase in awareness of these frauds but many companies are reviewing and formalising processes to handle such incidents.

Kent: The “Yates Memorandum” issued by the U.S. Department of Justice (“DOJ”) in September 2015 is an interesting development for both executives and corporations. Although it is not necessarily a departure from existing DOJ practice, it stresses that the government will seek more accountability from individuals who it believes have perpetrated corporate wrongdoing in both civil actions and criminal prosecutions. It lays out six steps to strengthen the DOJ’s pursuit of this goal:

- Companies must provide DOJ with all relevant facts relating to the individuals involved in the corporate misconduct in order to qualify for any cooperation credit;
- Criminal and civil investigations should focus on individuals from their inception;
- Criminal and civil DOJ attorneys handling corporate investigations should be in constant communication with each other;
- Generally, the DOJ will not release individuals from criminal or civil liability when resolving a matter with a corporation;
- The DOJ will not resolve claims against a company unless there is a “clear path” to resolve related individual cases; and
- Civil DOJ attorneys should consistently focus on individuals as well as the company, and should evaluate whether to sue individuals based on considerations beyond their ability to pay.

Blundell: There were two practical examples of how companies can avoid convictions by leveraging prosecutors’ incentives for self-reporting criminal conduct:

- In England, Standard Bank and the Serious Fraud Office agreed a Deferred Prosecution Agreement (DPA) after bribery of Tanzanian public officials. Standard Bank will pay out more than £32m in restitution and fines and appoint a monitor.
- In Scotland, Brand-Rex Ltd and the Crown Office agreed a Civil Recovery Order following bribery of suppliers. Brand-Rex will pay £212,800 to the Scottish government to resolve without a prosecution being commenced.

It’s hard to say whether the costs of the resolutions were higher or lower than the amount they would have been fined if they had been convicted – but in each case the company was able to “draw a line” under the issue and avoid incurring further legal costs, management disruption and reputational damage. That would have been particularly welcome for Standard Bank which was likely preparing to be acquired by ICBC at the time of the conduct.

Mansell: The first Deferred Prosecution Agreement (“DPA”) has received widespread publicity after considerable speculation about when it would come and who would be involved in it. On 30 November 2015 in SFO v ICBC Standard Bank U2015/0584, Sir Brian Leveson P, sitting in the Crown Court at Southwark, examined the agreement between the SFO and ICBC Standard Bank.

The case was carefully chosen: ICBC self-reported within days, fully disclosed its own internal investigation,
and co-operated throughout with the SFO. By the time the DPA was agreed, the bank was under new ownership and had undertaken a thoroughgoing review of its anti-corruption practices.

The court’s role under the new legislation, Sir Brian Leveson P was at pains to point out, is ‘pivotal’ (see [21]). This is a clear distinction from the approach in the United States. The statutory scheme on this side of the Atlantic, set out in s.45 and Schedule 17 of the Crime and Courts Act 2013, means that even if both parties (here, the SFO and the bank) are entirely ad idem, a DPA will only be approved once the agreement has survived close judicial scrutiny. This difference reflects concerns expressed by Thomas LJ in Sikellis v Innospec Limited in March 2010 as to the role of the Courts where prosecuting authorities seek to enter into plea agreements with corporate entities.

Sikellis: There have been a number of interesting developments in the white collar area. Among them is the important and now well-known issuance of the so-called “Yates memo”. Deputy Attorney General Sally Yates, issued a memo entitled “Individual Accountability for Corporate Wrongdoing” which sets the prosecution of individuals as a U.S. Department of Justice priority. Most significantly, under the Yates memo, companies will receive no credit for cooperation unless they disclose all relevant facts relating to individuals responsible for misconduct. This of course was likely in response to the overall drop in white collar prosecutions against individuals. For example, according to Syracuse University’s Transactional Records Access Clearinghouse (TRAC), the number of cases brought in the first nine months of 2015 is down 37% from levels seen two decades ago.

Internally, we merged our Compliance Legal and Compliance Investigation departments. This has led to a closer collaboration between lawyers and investigators and has also created more efficiency. Furthermore, we realigned our internal Compliance regulations and concentrated the rules as well as processes in one internal regulatory framework. This new global Compliance circular contains all company-wide regulations specifying the Business Conduct Guidelines provisions in the areas of anti-corruption, antitrust, anti-money laundering and data privacy as well as regulations regarding the Compliance Organization and binding topic-specific directives about applicable processes or the use of tools operated by Legal and Compliance. These, together with our Compliance Operating Model, constitute the Siemens Compliance System.

DiBianco: On 9 September 2015, the United States Department of Justice (“DOJ”) issued guidance, in the form of a Memorandum from Deputy Attorney General Sally Yates (“Yates Memorandum”), to its criminal and civil prosecutors that purports to change the Department’s approach to corporate investigations in order to facilitate individual prosecutions for corporate misconduct. While the focus on individual prosecutions is not new, the Yates Memorandum states that the DOJ will no longer give organisations “partial” credit for “partial” cooperation. Moreover, the guidance places new burdens on line prosecutors, who now must present a plan to investigate potentially liable individuals when seeking authorisation to resolve a case against the corporation, and must seek written authorisation to conclude an investigation without bringing claims or charges against individuals who committed misconduct. Moreover, the Yates Memorandum signals what may be a major shift in favour of the use of the Department’s civil enforcement powers against individuals. The Yates Memorandum could have particular impact on non-US companies involved in DOJ investigations, where local privacy and employment laws may limit the degree to which companies can cooperate with the DOJ in relation to conduct of individuals.

Jersey: Section 92 of the Care Act 2014 creates a new criminal offence for a provider organisation to supply, publish or otherwise make available certain types of information that is false or misleading where that information is required to comply with a statutory or other legal obligation. The offence applies to all NHS foundation trusts, NHS trusts and other organisations that provide care and treatment for the NHS. In certain circumstances, the offence can be committed by individuals. The offence came into force on 1 April 2015 and was introduced in response to the Public Inquiry into Mid Staffordshire NHS Foundation Trust. It forms part of the UK Government’s overall drive to improve the openness and transparency in the provision of health services.

Stetter: Recently there have been a number of regulatory changes and interesting developments in Germany. The most important ones are the following:

Effective as of 26 November 2015, Section 299 of the German Criminal Code
sanctioning commercial bribery has been significantly revised and expanded.

The revised provision makes the request, acceptance of a promise for or acceptance of an advantage, a crime if this is made: (i) in return for providing an unfair advantage in a business competition, or (ii) in return for a breach of duty towards the commercial organisation. Likewise, the offering, promising or granting of a benefit to an employee or an agent of a commercial organisation is a crime if made: (i) in return for obtaining an unfair advantage in a business competition or (ii) in return for a breach of duty towards the commercial organisation. Prior to the revision, active and passive commercial bribery was only punishable under criminal statutes when the corrupt conduct was connected to unjustified preferential treatment in the context of a competitive transaction. In particular the interpretation of the new relevant element of the provision, the “breach of duty towards the commercial organisation” is still subject of discussion. There is uncertainty, for example, as to which specific acts would qualify as a breach and thus fulfil the elements of the crime.

Furthermore there is another important regulatory change concerning corruption in health care about to be implemented:

The practice of pharmaceutical companies, particularly through their sales persons, to give out complimentary gifts and benefits to private practice doctors in the form of medical devices, junkets or other forms of award has been under scrutiny. The granting of gifts and benefits to private practice doctors had fallen out of the ambit of the relevant statutes of the German Criminal Code. So as to provide a more consistent standard to this sector a bill of law has been drafted stipulating new offences within the meaning of bribery, and specifically bribery in the health sector. The draft legislation has generally been met with approval, even though ambiguities concerning the delineation of punishable scope and criminal behaviour have led to complaints. It is likely that the legislation will enter into force in the course of 2016.

Another regulatory change concerns “revolving doors”:

The practice of politicians and senior public officials transferring over to rewarding positions in the private sector has been under scrutiny for a considerable time. Such cases have often been reported in the press and subsequently frowned upon. As a result, new legislation has been introduced that entered into force in July 2015. It defines a transition period of between 12 to 18 months before current and previous members of the government who wish to move out of public service can take up positions in the commercial or private sectors. That current or previous member is also obligated to notify the government about their intentions to move elsewhere. This provides the government with the option of disallowing the request thereby leading to considerations of monetary compensation should an official be denied approval to take up a post. Critics of this type of ‘governmental self-control’ contend for fixed waiting periods of up to three years and extension of the rule to other groups of persons.

Zimiles: First, earlier this fall, the Department of Justice issued the Yates Memo, which set forth the standards that companies must satisfy to obtain cooperation credit in corporate prosecutions. The Yates Memo also contains the principles that DOJ attorneys would be required to follow as a means of ensuring that where appropriate, individual employees would be held accountable for corporate wrongdoing. In addition, DOJ also recently appointed a compliance counsel who will help assess a company’s program and determine whether it is “thoughtfully designed and sufficiently resource to address the company’s compliance risks, or essentially window dressing.” The compliance counsel will also help guide prosecutors in determining the nature and scope of any sanctions against the company.

2. Can you outline the key fraud and white collar crime trends in your jurisdiction?

Mackenzie: We are seeing cyber-crime as the emerging trend that causes us the most concern. It would appear that cyber-crime is badly under-reported and much of the analysis is focused upon cases such as the theft of personal data at major companies, such as the 2014 cyber-attack of Target. However, it is SMEs that are often the most at risk as they are unlikely to have the infrastructure or personnel to respond. A recent incident that we have seen has highlighted this. In this matter a staff member opened an email with ‘crypto-locker’. This software encrypted all of the business’ data unless certain payment was made. The result is that the SME was unable to trade until the crypto-locking. In addition, DOJ also recently appointed a compliance counsel who will help assess a company’s program and determine whether it is “thoughtfully designed and sufficiently resource to address the company’s compliance risks, or essentially window dressing.” The compliance counsel will also help guide prosecutors in determining the nature and scope of any sanctions against the company.
was dealt with.

The key learning in this case was that the SME had a relationship with their insurer that provided the relevant IT expertise to advise on how to deal with the crypto-locker and to meet the costs associated with the business interruption.

Kent: In the U.S., civil and criminal investigations regarding federal contracts and alleged procurement fraud have remained consistent. There has been somewhat of an increase in activity in the investigation of alleged fraud in federal programs designed to enhance the involvement of minority and women owned businesses in federally subsidised contracts. In Pennsylvania and New Jersey especially, where my practice is primarily based, there has been a focus for many of the last several years on the conduct of public officials, including not just the executive branch but also the judicial and legislative branches as well. In England, there has been a marked increase in the number of Bribery Act prosecutions brought by the Serious Fraud Office. Lastly, one of the areas in which we focus is compliance with and litigation concerning the federal E-rate program, known officially as the Schools and Libraries Program of the Universal Services Fund. There were several criminal investigations and False Claims Act litigations against technology companies that arose from the rounds of E-rate funding years ago. Now that there has been a new round of E-rate funding made available to school districts and libraries, we expect another increase in such cases.

Blundell: Corporate clients face two trends that are pulling in different directions: sophisticated white collar crime is being detected and prosecuted better than ever before. Specialist prosecutors have achieved some great successes around the bribery of foreign officials and manipulation of financial markets: in particular, the 14 year prison sentence (recently reduced by the Court of Appeal to 11 years) given to financial trader Tom Hayes for LIBOR manipulation has been a huge wake up call for financial institutions and employees alike.

At the same time, it’s harder than ever to get real assistance from law enforcement and prosecutors to investigate fraud where companies are the victim. Corporate clients are turning to us to conduct criminal investigations and bring private prosecutions because the public sector is so overstretched.

Mansell: In a speech to the Cambridge Economic Crime Symposium in September 2015, David Green CB QC gave an overview of the SFO’s direction of travel. He had given a similar kind of speech to the Pinsent Mason Regulatory Conference a year before in October 2014. Current trends from an SFO perspective are:

- DPAs gathering momentum;
- increased co-operation with the US Department of Justice;
- an explosion in cyber-fraud; and
- a move away from the identification principle, which for corporate offending has caused prosecuting authorities serious problems.

Libor has been a live issue for some time now, but August 2015 saw the first conviction after trial: Tom Hayes was found guilty of eight counts of conspiracy to defraud before Cooke J and a jury at Southwark Crown Court; in December, some months later, the Court of Appeal reduced the heavy sentence imposed on Mr Hayes to 11 years’ imprisonment, see R-v-Hayes [2015] EWCA Crim 1944. Looking forward, then:

- this first successful and high-profile conviction lends credibility to the SFO’s ability to prosecute complex Libor offences, where initially this was in doubt;
- a raft of Libor prosecutions are now following close behind Tom Hayes’ conviction: the second trial (of six brokers from ICAP, RP Martina and Tullet Prebon) began in October and will be closely followed by a trial of defendants from Barclays Bank.
- The SFO is also turning its attention to the alleged manipulation of EURIBOR and prosecutions for FOREX are in the pipeline.
- the Court of Appeal has made it clear that 14 years in prison will be far from the maximum sentence for this kind of offending: Lord Thomas CJ warned those in the City of London that on the contrary terms of imprisonment for conduct of this kind could, in future, be ‘significantly greater’ (at [109]).
- The SFO is continuing its charm offensive to dilute the “directing mind” test for corporate criminal liability.

DiBianco: In the area of Foreign Corrupt Practices Act (“FCPA”) enforcement, the U.S. Department of Justice (“DOJ”), with only two corporate enforcement actions in 2015, was at its lowest corporate enforcement level since 2006. Moreover, the overall monetary value of the 11 FCPA enforcement actions handled by both the DOJ and the U.S. Securities and Exchange Commission
totalled $139 million, which is down significantly from prior years. By way of comparison, in 2014 and 2013, the total amount paid was $1.56 billion and $731.1 million, respectively. Even so, the DOJ and SEC both have publicly indicated that the commitment to FCPA enforcement is stronger than ever, with DOJ reporting that it has increased the number of agents and prosecutors dedicated to FCPA cases. Government officials report that they are focusing on larger and more complex matters that are time consuming to investigate and resolve. Public filings indicate that, as of the end of the 2015, more than 80 companies had reported some form of unresolved FCPA-related investigation, and additional companies face internal or government investigations that have not been reported. In addition, the increased number of reported tips to the SEC’s Whistleblower Program inevitably ensures an almost steady pipeline of potential enforcement actions in the future.

Jersey: 2015 has seen the UK’s Serious Fraud Office (“SFO”) agree its first Deferred Prosecution Agreement (“DPA”) since their introduction in February 2014. Standard Bank Plc entered into a DPA with the SFO in respect of an allegation of failure to prevent bribery by two executives contrary to Section 7 Bribery Act 2010. This case was also the SFO’s first concerning the corporate offence of failure to prevent bribery. The second DPA is expected imminently. Whether this sees the start of a flood of DPAs remains to be seen however given that the UK Government has shelved plans to create a corporate offence of failure to prevent fraud; a trickle seems more likely.

Stetter: Probably one of the most important trends, if not the most important trend, in white collar crime is the ongoing reform of private sector bribery offences. There has been criticism of Section 299 of the German Criminal Code as it was perceived as falling short of the standards that Germany signed up to under the Convention of Corruption of the Council of Europe. Until 2015 Section 299 only covered bribery specifically in relation to market competition. As Germany was anxious not to be seen to be behind the curve of international standards, it moved quickly to rectify this. The new provision, as described in answer to question 1 above, goes beyond just market competition, stating that it shall likewise be a criminal act to offer, promise or grant (and the same for passive bribery) an employee or agent of an enterprise a benefit for himself or herself or another ‘for violating his duties vis-a-vis the enterprise’ while procuring goods or commercial services. This development underlines the overall trend of ongoing efforts to identify and eliminate legal grey areas in the field of white collar crime in Germany.

Ratley: Information security and technological innovations are two major trends to keep an eye on in the near future. Information security is a major concern for organisations of all sizes and in virtually every industry, especially in the wake of the numerous high-profile data breaches that occurred in 2015. These breaches show that senior executives must become more aggressive in strengthening information security and preparing for potential breaches. Also, technology will continue to play a key role in shaping the fraud landscape. Fraudsters are becoming more innovative in their use of technology and, consequently, their schemes are growing in complexity. These developments mean that anti-fraud professionals must also adapt to advances in technologies.

Zimiles: The fraud and white collar crime trends continue to be the traditional crimes observed in previous years but with the added complication however that these crimes are increasingly being facilitated through advancements in technology. Hackers have gained access to consumers’ bank and brokerage funds – illegally trading through those accounts and stealing funds. Additionally, digital currency such as Bitcoin has given criminals a new way to mask their identity. And, individuals use shell companies and third parties as a means of obfuscating illegal activity, whether it be corruption, drug and human trafficking, embezzlement or insider trading.

3. What impact has U.S. v. Newman had in terms of the prosecution of insider trading?

DiBianco: Following the decision, prosecutors in the Southern District of New York dismissed charges against Michael Steinberg, a former portfolio manager at hedge fund S.A.C. Capital Advisors LLC. The SEC also decided not to pursue civil charges against Mr. Steinberg. In January 2016, Steven A. Cohen agreed to a two-year prohibition on supervising funds that manage outside money until 2018 in order to settle SEC charges that he allegedly failed to supervise a former portfolio manager at a wholly owned subsidiary of SAC. The resolution with Mr. Cohen is less stringent than was expected before the Newman resolution and appears to reflect the challenges that the SEC
would face in pursuing a case that he failed to supervise traders where there is not clear evidence that tipped information was provided to the traders in exchange for potential pecuniary gain or similar value.

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

Kent: With regard to the Foreign Corrupt Practices Act (“FCPA”), recent SEC enforcement actions highlight that the scope of the FCPA extends beyond government employees to political party officials and to employees of “public international organisations.” Hitachi Ltd. recently resolved a civil enforcement action premised on allegations that it engaged in improper transactions with a front company for the African National Congress. Similarly, earlier this year the DOJ brought criminal charges against a consulting company executive for allegedly improper consulting payments to the relative of an executive for allegedly improper conduct against a consulting company. This is an especially useful case for the FCA in its efforts to hold corporates accountable for the actions of traders. Further, it distinguishes market abuse from criminal market offences where not only is a mens rea required, but for corporate accountability to attach it would be necessary to establish wrongdoing by the company’s ‘directing mind’.

For market abuse, the Court looks at the behaviour and its effect. For corporate liability to attach the Court will look at a company’s rules of attribution (normally found in its own constitution) and will apply the law of agency. This approach builds on the Privy Council’s decision in Meridian Global Funds Management v Securities Commission [1995] 2 AC 500 and, more recently, the Supreme Court’s decision in Jetivia SA v Bilta Ltd [2015] UKSC 23.

DiBianco: In the FCPA area, pursuit of individuals (rather than corporate settlements) continue to generate litigation of FCPA elements and procedural rules. In United States v. Laurence Hoskins, 3:12-cr-00238-JBA (D. Conn. 2015), the United States District Court held that Hoskins, as a non-resident foreign national who was not an agent of a domestic concern and did not commit acts while physically present in the territory of the United Sates, could not be subject to criminal liability under the FCPA under a theory of conspiracy or aiding and abetting a violation of the FCPA by a person who is within the statute’s reach. The DOJ has moved for reconsideration of the court’s ruling. Moreover, United States v. Sigelman, 14-CR-00263-JEI, (D.N.J. 2015), provides insights into the aggressive tactics prosecutors are attempting to utilise to pursue FCPA cases, including undercover informants and secret video/audio button recording devices.

Jersey: The first DPA was approved by Lord Justice Leveson on 30 November 2015. The prosecution was deferred for a period of three years, required Standard Bank to pay a total of $4.91m in financial orders and be the subject of an independent review of its existing anti-bribery controls. In his judgment approving the DPA, the Judge emphasised that the Bank had self-reported within days of identifying the wrongdoing and fully co-operated with the SFO. The Judge also emphasised that these factors allowed for a full reduction of one third in respect of the financial penalty imposed. It is clear from this Judgment that the cooperation by a corporate is a key factor when deciding whether a DPA should be entered into.

5. What are the benefits and disadvantages in using court experts and expert witnesses?

Kent: Experts can be a significant advantage when they can credibly distil complicated concepts into plain English for the fact finder. In addition, an expert’s depth of knowledge in a relevant subject area can often help your lawyers identify additional or alternative legal and factual themes that are not initially apparent to a non-expert in their field. The major disadvantage of an expert witness is cost—usually pay for quality. In addition, in some cases experts effectively “neutralise” each other, contributing to some clients’ frustrations with the costs of the U.S. legal system. Overall, in my experience the advantages of expert testimony in complicated technical matters generally outweigh the disadvantages.
The real key is adequately vetting any potential expert.

**Blundell:** Expert evidence can be a powerful tool for a litigant: they can cut through confusing factual matrices and present evidence in a way that’s accessible to the judge and/or jury. We have had particular success with experts that use presentation tools (e.g. diagrams, 3D modelling and animation) instead of relying only on the spoken word and written affidavits.

The main disadvantage is obviously cost: skilled expert witnesses are expensive. They often require extensive briefing and preparation time, and they may request large volumes of data or documents. Also, expert witnesses can’t be required to come to favourable conclusions – or even any conclusions! We have certainly seen instances where the expert was unable to form any definite opinion about the subject matter and did not ultimately give evidence – but the litigant paid their fees in full.

**Mansell:** It is as important as it has ever been in the criminal jurisdiction not to take it for granted that just because an area is difficult (even technically difficult) then expert evidence will be required or even admissible. In Libor cases, for example, the Court of Appeal is clear that a jury considering the objective limb of the Ghosh test is to rely on its individual members’ knowledge of the world rather than on an independent expert: *R v Tom Hayes [2015] EWCA Crim 1944*, at [32].

Some benefits of expert witnesses are that:
- they are often (although not always) capable of bringing clarity and coherence to other technical evidence which would otherwise remain in comprehensible;
- there is now much better training for expert witnesses than there once was, so they increasingly know what they are doing even if relatively inexperienced;
- they can be instructed at an early stage to assist with narrowing the issues and providing comprehensive advice; and
- Part 19 of the Criminal Procedure Rules is now likely to save some time at trial by encouraging (i) the instruction of a joint expert or (ii) pre-hearing discussion between experts if there is more than one.

The disadvantages may be that:
- an expert’s primary duty is to the court rather than to the client, so there is no guarantee how advantageous their evidence will be to a client’s case;
- the cost implications for a privately paying client can be substantial and sometimes unwelcome;
- some experts bury the jury in a mass of complicated information and do not in fact assist them at all; and
- experts occasionally give unexpectedly damaging evidence or can too easily change their view, particularly under the pressure of cross-examination.

**Jersey:** Whether expert evidence is required in defending criminal cases depends on a number of factors, in particular whether the prosecution is reliant upon expert evidence. An expert witness are under a duty to the court to provide an objective and independent opinion on matters outside the experience or knowledge of a jury irrespective of any obligations owed to the party instructing them. Having obtained a defence expert report there is no currently no requirement on the defence to serve a report if there is no intention to rely upon that expert, for example because they assist in some areas but are not as helpful in others. In this situation often an expert report can provide assistance in cross-examination of other witnesses.

**Ratley:** Financial crimes can be among the most complex court cases, and attorneys often need the help of experts not only to develop the case, but also to potentially explain it to a judge and jury. A case might need technical analysis or call on the court to decide whether a professional standard was violated, and this is very difficult to do without the guidance of a respected expert in the relevant field.

On the other hand, parties typically have to reimburse the expert (or multiple experts) at a substantial hourly rate and pay for travel expenses. The expert might be required to appear in multiple depositions or proceedings. In short, it can get expensive. In cases with small amounts in controversy, expert testimony often is not feasible. Even in major litigation, parties have hired experts when doing so was not necessary to prove the case effectively. This mistake could confuse the jury, or the court may refuse to admit the expert testimony.

**Zimiles:** Perhaps the biggest benefit of an effective expert is that if the expert opinion is accepted, there is more credibility to the point being made than if a lay witness had tried to make the same point. On the other hand, a paid expert who is painted as hired gun or mercenary potentially demeans...
On alleged misuse of federal funds through the federal False Claims Act (FCA). Not only does the FCA provide whistleblowers with an attorney’s fee award and as much as a 30% share in a recovery that may include treble damages, but it also provides employee and contractor whistleblowers with substantive protections against retaliation and a private cause of action for retaliation. The IRS and SEC have whistleblower programs with similar protections and incentives in matters involving tax fraud and securities law violations, respectively. It is important not to overlook the myriad state laws that offer varying degrees of protections for whistleblowers as well. Several of those laws provide specific additional protections, especially for employees of businesses that receive state funding, including damages and attorneys’ fees awards.

**Blundell:** Whistleblowers have good, but not great, protection in the UK. At its core, an employee must not suffer detriment because s/he makes a good faith disclosure about of criminal/un- safe/unjust conduct.

Employers often overlook the value of whistleblowers in detecting white collar crime/fraud. It’s much cheaper, quicker and less embarrassing to find out about potentially unethical conduct from your own employees than it is to find out about it from law enforcement when they turn up to raid the premises.

There are no incentives for whistleblowing in the UK. However, many of our clients are subject to the Sarbanes-Oxley and Dodd-Frank regimes, under which whistleblowers can earn multimillion dollar bounties if employers ignore them. It is another reason for corporations to encourage whistleblowers to come to them first, and respond appropriately.

**Mansell:** The principal domestic legislation protecting whistleblowers in this country is contained within the Employment Rights Act 1996 (ERA 1996), as amended by the Public Interest Disclosure Act 1998 and (some years later) by the Enterprise Regulatory Reform Act 2013. The ERA 1996, so amended, provides that if a ‘worker’ makes a ‘protected disclosure’, he or she should not as a result be subjected to any detriment by his employer (s.47B); furthermore, any dismissal that results (if the disclosure is ‘the principal reason’) will be an unfair dismissal (s.103A). Some further definitions are important:

- A ‘protected disclosure’ is a qualifying disclosure within the meaning of s.47B(1)(a)-(f), i.e. disclosure of information which, in the reasonable belief of the worker making it, is (i) made in the public interest and (ii) tends to uncover, for instance, a criminal offence, a miscarriage of justice, or a health and safety scandal.

  - The word ‘worker’ is now very broadly construed: the Supreme Court held in Winkelhov v Clyde and Co. LLP [2014] UKSC 32 that the legislation protected a partner in a solicitors’ firm who reported money-laundering in a joint venture in Tanzania.

There is at present no system in place to provide financial incentives for whistleblowers in way exemplified by the American regulators. The FCA and the PRA reported to the Treasury Select Committee in 2014 expressing their serious reservations about the how successful the US model had really been and explaining their concerns about the potential dangers of such incentives, which in their view included malicious reporting, entrapment, and public perception.¹ They appear to remain resolute in that view.

**Sikellis:** Siemens expects its employees to report all information they may have regarding impending or ex-

---


---
isting compliance cases without delay. In this connection Siemens does not favour incentive models. Siemens counts on voluntary reporters who are not driven by a commercial hidden agenda. Employees may report compliance cases to their supervisors and/or the relevant Compliance Officers or directly to the Chief Counsel Compliance or the Chief Compliance Officer or any other member of the Legal and Compliance Organization. Employees may also use the protected reporting channels “Tell Us” (a secure and 24/7 IT tool where reports can be sent if favoured anonymously) and the Ombudsman. Whistleblower protection is taken very seriously at Siemens and retaliation of any kind against individuals who have reported compliance cases is not tolerated. This prohibition applies to a broad range of actions that may directly or indirectly harm the employment relationship, earning potential, bonus payments, career development or other work-related interests of the reporter.

DiBianco: The U.S. Securities and Exchange Commission’s (“SEC”) current whistleblower program was created in July 2010 following enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act. Where a whistleblower provides original information that leads to a successful SEC enforcement action and monetary sanctions total over $1 million, the SEC can award a whistleblower between 10% to 30% of the monetary sanctions collected. Whistleblowers are protected from retaliation for providing information to or assisting the SEC. The anti-retaliation provisions extend to those who report concerns internally but are terminated before they have an opportunity to go to the SEC. Since the program was established, the SEC has paid more than $54 million to 22 whistleblowers, with more than $37 million paid in fiscal year 2015. The SEC reported that it received nearly 4,000 whistleblower tips in fiscal year 2015, which is 30% more than in fiscal year 2012.

Jersey: The Financial Conduct Authority introduced new rules on whistleblowing that apply to banks and insurers in early October 2015. The new rules have numerous requirements that relevant firms need to put in place including: the appointment of a Senior Manager as their whistleblower’s champion; implement internal whistleblowing arrangements; inform UK based employees about the whistleblowing services; present an annual report to the firm’s board and notify the FCA if it loses an employment tribunal proceeding with a whistleblower. The requirements introduced by the FCA shows that the FCA considers more work is required in this area and continues to encourage whistleblowing. The FCA has however not taken any steps towards introducing US style financial incentives for whistleblowing.

Stetter: In Germany, in relation to whistleblowing, there exist no such well-developed incentive systems as in the area of Anglo-American law. However, whistleblowing has been occurring specifically in the context of companies and law enforcement and is not to be underestimated in its importance.

According to the federal status index of the German Federal Office of Criminal Investigation 2013, 60% of all corruption connections had been in existence longer than three years. So year after year there are a large number of offences that are committed under the radar of the competent authorities. That is why criminal investigation authorities are reliant on corporations’ own compliance systems and whistleblowing in particular. In 2013, more than two-thirds of legal proceedings in this regard were instigated based on such information being received.

This proportion continues to grow because more and more companies are implementing detailed compliance guidelines and internal whistleblowing systems.

Ratley: Whistleblower laws in the U.S. are fragmented—they differ based on jurisdiction, industry, and sector. The protections available to a federal employee might be very different from those to, say, an employee of a private manufacturing company. This complexity and the fear of retaliation can have a chilling effect on whistleblowing. However, the general trend over the past several decades has been for greater protection. Legislatures have recently passed laws creating or increasing financial incentives for whistleblowing (e.g., programs by the Securities Exchange Commission and the Internal Revenue Service).

In the private sector, a modest number of organisations provide financial incentives for whistleblowing. More commonly, organisations encourage whistleblowing by promoting an anonymous hotline where employees, contractors, customers, or others can report fraud and other violations. We know from our study on occupational fraud, The Report to the Nations, that tips are by far the most common de-
tection method for internal fraud. Organisations are increasingly taking advantage of tips by facilitating whistleblowing.

Zimiles: There are various U.S. whistleblower statutes, rules and regulations, including, but not limited to Section 922 of the Dodd-Frank Act and the U.S. False Claims Act. Generally, the various regulations provide financial rewards to individuals who provide information which results in a successful enforcement action or prosecution against a wrongdoer. To encourage the free flow of information regarding potentially illegal or unethical activities, whistleblowers are also provided with anonymity and federal law prohibits retaliation against them for providing such information. Corporate compliance programs should contain documented procedures instructing employees to anonymously report any potentially illegal or unethical activity to their supervisor, human resources, or the compliance or legal department.

7. How can data and analytics be utilised for a more effective risk management procedure? What else should be included in a company’s risk management framework?

Mackenzie: Risk management should really begin at board level and not just be considered an IT or compliance issue. Once the board has embraced the importance of managing cyber risk, then this can be driven across all parts of the business through a holistic approach to risk management, including risk mitigation and loss response. Whilst we often work with our clients on reviewing detection and procedures to prevent fraud, it is all too often that too little focus is placed on response plans for when fraud occurs.

The response that many fraud experts offer when asked about the possibility of a major fraud occurring is “it is not if, but when”. Given this bleak view, companies should consider implementing a response plan to deal with a major fraud. Key to this will be what legal, forensic accounting, public relations and insurance advisors will be engaged.

Once in place, such response planning should be tested annually through the use of table top exercises to identify gaps in the plan.

Kent: Data analytics can be effectively employed to detect questionable activities that would not necessarily raise questions as isolated acts, but that collectively may appear as a pattern that raises red flags requiring further investigation. For example, spending patterns of sales divisions that show spikes in spending on entertainment of personnel involved in federally funded programs could be such a pattern. Similarly, data analytics can make use of keywords, phrases, conceptual compilations and/or financial patterns to formulate a “profile” of an issue requiring further human assessment for regulatory risk. Larger companies that have the financial wherewithal to implement and enhance the use of data analytics should make it a key component of their compliance programs, as the lack of its use could have substantial negative ramifications both for detecting improper conduct and for defending the company in legal matters premised on that conduct.

Sikellis: Big data is certainly a main topic of conversation these days. Also for Compliance a mass of data is produced daily from its own processes and in relation to compliance relevant transactions within the company. The convergence of data together with easy data visualisation has opened up endless possibilities to use data beyond classic reporting. Particularly in the field of risk, data analytics in combination with data visualisation can be used to greatly support the risk management & mitigation process. Nevertheless, obtaining meaningful data and being able to structure the data are key areas that still have to be considered to make it a success. This solved the definition of risk analytics will shift the focus from a process driven to a transactional driven risk analysis. Focus on the transactions will still highlight process weaknesses, that can be remediated, but at the same time it allows deeper insight into potential risks otherwise not addressed.

The important point is that no one analytic will equal a red-flag, but it’s the combination of analytics or alerts that can be considered to highlight potential risks. For example, using Business Partner tool data, could uncover: a business partner sitting in a high risk country, in a cross-border situation, dealing with government, having less than five persons, no physical compliance officer in-country and so on. But then further adding supplement data from other sources, e.g. Dun&Bradstreet data to check company size, or SAP data to get an understanding of payments to the business partner etc. Data analytics obviously compliments a top-down / bottom-up risk analysis as part of the annual Compliance Risk Assessments. Something that is important to capture the “risks” not in tool data. Basically, the experience and knowledge is...
of persons not in “digits”.

DiBianco: Data analytics examines raw data with the goal of drawing conclusions from that data and can provide significant potential in the area of risk management. Data analytics can be used to examine historical data to identify and quantify potential errors that may have occurred in the past. It can also be used to provide current, ongoing monitoring and forward-looking analysis of potential developments. In terms of an organisation’s overall compliance program, data analytics can be an invaluable tool in assisting an organisation to meet the requirement in the Corporate Sentencing Guidelines to continuously monitor and assess the effectiveness of its compliance program. In addition to data analytics, an organisation’s risk management framework should provide for an effective avenue to resolve identified risk promptly to ensure ongoing compliance.

Ratley: In the age of big data, companies must harness the power of their data to effectively manage their risks, especially the risk of fraud. To do so, both the fraud risk management program and the data analysis process must be based on a thorough and living risk assessment. The company must identify where it is most vulnerable to fraud and then implement an analytics framework that digs through the data to find the red flags of those risks. Additionally, as the amount of data companies have grows, the use of predictive analytics techniques—where the data itself defines what is normal and uses that to identify outliers—helps catch frauds more quickly and mitigate the associated losses.

Zimiles: The concept of a “risk-based” approach to compliance has made the effective use of data and analytics extremely important. Specifically, in the area of anti-bribery and corruption compliance, more and more companies are collecting and analysing information about third-party business partners to identify, assess and investigate the potential risks associated with such relationships. In addition, in the area of anti-money laundering compliance, former New York State Department of Financial Services Superintendent consistently emphasized the need for financial institutions to ensure that their transaction monitoring systems were sufficiently robust.

8. What advice would you give to an organisation undertaking an internal investigation when serious misconduct is suspected?

Mackenzie: There is often a complex mix of legal, employee and other commercial considerations that may need to be considered in balancing how the company conducts the investigation. In most cases, the company should engage external advisers, including legal, forensic accounting, public relations and insurance advisors.

However, ownership must be retained and driven by the company’s executive. Far too often, it would appear that there is not sufficient executive ownership where there is serious misconduct suspected and, all too often, the company’s executive only become involved when the matter has become public.

Kent: At the first sign of a potential material violation of law, the company should engage qualified counsel, and immediately implement data preservation measures, as instructed by counsel. Careful analysis should be given to whether employees/executives potentially involved in the underlying conduct need separate representation, and whether they should or must be indemnified for legal expenses. In the nascent stages of the investigation, in-house lawyers should avoid substantive discussions with such personnel without guidance from outside counsel. At a minimum, in-house lawyers should be clear about the fact they represent the company, not the executive, and accordingly that the substance of their discussions is not subject to a privilege held by the employee/executive, but rather by the company. Careful consideration should be given to whether in-house lawyers may have had knowledge of or involvement in discussions about the conduct being investigated, and whether they should be screened from involvement in the investigation to preclude questions about its objectiveness (as well as for their own protection). Lastly, care should be taken regarding the handling of the source of information leading to the investigation – when that source is an employee, and sometimes when it is a contractor, the source may qualify as a whistleblower and correspondingly for the various protections afforded to whistleblowers.

Blundell: The two critical values of internal investigations are timeliness and fairness. Timeliness means responding without undue delay: as time goes on, memories fade, documents are lost and positions become entrenched. Equally, getting the benefit of self-reporting means acting promptly. However, a timely response should never be a rushed response.
At the same time, fairness means ensuring that the investigation is structured properly: that all topics that should be examined are properly addressed; that the subjects of the investigation are treated with dignity; that the investigators are objective and impartial to the outcome; and that all of these things are properly documented so they can be demonstrated to employees’ counsel, regulators and law enforcement in the future.

Mansell: This is an enormous subject and in each case specialist advice is required. Some key issues to consider:

- Who should conduct the investigation and what the purpose of it is.
- The employment position of individuals and whether and when they should have access to their own legal advice.
- Be alive to the risk of contamination: think about what information barriers might be necessary, and give serious thought in particular as to whether to interview, who to interview and the chronology of interviews.
- Legal Privilege is a highly complicated and constantly changing aspect of internal investigations. Be alive to the risk that documents may have to be disclosed. Do not disseminate sensitive material any more widely than it needs to be. Recognise that privilege will not attach to all individuals in the organisation. If necessary, instruct lawyers to advise on privilege; establish clear communications lines.
- Be very careful with notes of interview. They are unlikely to be covered by legal advice privilege in a pure form, and although they might be covered by litigation privilege, the SFO/FCA are increasingly challenging these claims (particularly with interviewees’ first accounts): the signs are that in due course the SFO/FCA may start litigating in this area in the higher courts.
- Consider if the law requires wrongdoing to be reported, or whether notification is desirable in particular: (i) the obligations placed on companies and individuals by the Proceeds of Crime Act 2002 and the Money Laundering Regulations 2007; (ii) consider corporate exposures e.g. adequate procedures which must be in place to prevent bribery under s.7 of the Bribery Act 2010 and (iii) the risks and consequences of not reporting.
- Assess whether (and if so when) an external law enforcement agency needs to be brought in. Sir Brian Leveson P’s judgment on the first DPA demonstrates how important it is to act expeditiously.

Sikellis: There are many components to conducting a proper internal investigation. First and foremost is the need to ensure an objective and impartial investigation. The integrity of the investigation is of paramount importance. Know the law. All people involved in conducting the internal investigation and fact-finding must perform their duties in a manner which is consistent with applicable laws and company values. Ensure there is no retaliation against whistleblowers. Maintain confidentiality. It is important that the identities of the complainant, witnesses or the subject of the investigation not be disclosed to third parties unless required by law. Internal inquiries regarding ongoing investigations must be handled according to the “need-to-know principle”. Make sure the evidence gathering process is handled properly and in accordance with all legal requirements and company values. These principles ensure that all investigations are conducted in accordance with the confidentiality requirements and the law within each jurisdiction. In short, internal investigations must be handled by experienced people, there are just too many pitfalls.

DiBianco: Timeliness and the manner in which the organisation structures its internal investigation is vitally important where serious misconduct is suspected. Of particular concern is whether the suspected misconduct potentially implicates multiple jurisdictions. In this regard, the organisation should engage experienced outside counsel early in the process to advise on an appropriate investigation plan that addresses associated risks presented by the nature of the misconduct and the jurisdictions at issue, including risks in the areas of data preservation and collection, interviews of relevant individuals, fact analysis and reporting, and disclosure obligations. An organisation that does not appropriately structure and conduct its internal investigation of serious misconduct can end up in a demonstrably more negative position than if the investigation was not launched in the first instance. On the other hand, a timely, carefully managed, thorough, and objective internal investigation can positively shape how regulators perceive the Company and its overall commitment to ensure ongoing compliance.

Jersey: The aim of an internal investigation should be one of fact finding namely to determine what has happened. At the outset it is important to set out clearly the scope of the investigation, what its objectives are and what resources are required. Material relevant to the investigation must be identified and secured quickly with a clear
documented process. Issues such as what may be covered by legal professional privilege need to be examined, particularly if the investigation covers different jurisdictions as different rules of privilege will apply. Consideration must be given to what regulatory or other notification requirements may apply. Consideration should also be given to whether employees who are suspected of serious misconduct should be suspended and offered independent legal advice as part of the interview process.

Stetter: Very often it is extremely important for such an organisation to get a thorough understanding of all the potential risks as soon as possible, even if it means gaining such an understanding whilst the document review is still ongoing and thus being that the analysis can only be based on a preliminary understanding of the facts or a worst case scenario analysis. Once the potential risks are better understood at the very least a general understanding of the overall strategy of the organisation should be developed, the organisation is in a position to decide on specific issues in particular as to how to deal with subpoenas and approaches from law enforcement.

This approach enables the organisation to:
- conduct the investigation as efficiently as possible,
- gain more control as speedily as possible and
- implement the developed strategy as quickly as possible.

This all leading to its better protection.

Ratley: Ideally, an organisation will already have a team identified for investigating certain types of misconduct before it happens. For some organisations, this will mean outsourcing investigative duties. There are special concerns for investigations that involve executives or owners (common in major frauds). In these cases, it might be best to obtain outside legal counsel, due to privilege issues that can arise. Additionally, outside investigators and legal counsel help ensure that an objective inquiry occurs. Confidentiality is also an important goal for serious misconduct, and having a selected fraud team planned beforehand helps to only provide case information on a need-to-know basis.

Zimiles: The Department of Justice has always expected that internal investigations be thorough, tailored to the scope of the wrongdoing and that their intended purpose is to uncover the wrongdoing and wrongdoers regardless of their position, status or seniority in the company.

To that end, an organisation’s compliance program should include documented internal investigation protocols that address matters including, but not limited to preservation, collection and analysis of documents, preparing for and conducting employee interviews, internal and external communications regarding the matters, when to retain outside counsel and investigative and forensic experts and considerations for making voluntary disclosures to the government.

9. Can you talk us through the process of damage limitation for an organisation whose cybersecurity has been breached?

Mackenzie: When discussing response, the key to success is to rapidly engage professionals to determine whether a breach has occurred and to complete a preliminary assessment so that a loss control process can be quickly mapped out. For those businesses that have purchased cyber insurance, their insurer should be able to provide professionals that can offer quick solutions and rectification, often meaning the damage can be mitigated.

The preliminary assessment should be completed as quickly as possible, particularly if there may have been a data theft. Key questions include:

- What is the data, and does it contain third party and/or personal data?
- What is the likelihood of disclosure?
- If the data is disclosed, what are the potential commercial and legal damages?
- What other losses, such as business interruption, reputational damage or potential extortion, could be incurred?
- Are there legal obligations to notify regulators or third parties that need to be considered?

Only at this point can a company formulate a full strategy to limit damage. In a number of examples we have seen, the damage to the company has not necessarily been legal, but rather the reputational damage caused by not being forthright with third parties whose data has been compromised.

In terms of the legal requirements, the latest Australian exposure draft of the Privacy Amendment Bill has identified that affected third parties must be notified as soon as practicable and no longer than 30 days after discovery.
Once the organisation has established the scope of the loss, a review should be completed to improve the organisation’s cyber risk management and improve the company’s resilience in the event of future matters. It is all too often that an organisation suffers further breaches, having not learned the lesson the first time.

**Blundell:** Cybersecurity is a specialist field, but limiting the damage resulting from a cybersecurity breach is a multidisciplinary effort. Organisations will respond most effectively when they are all pulling in the same direction. Employees and advisors in IT, legal, regulatory affairs, crisis PR, investor relations and customer service all need to know what the other is doing. In crisis management, there is no substitute for planning.

Most importantly, organisations need to keep talking to stakeholders: to investors, to insurers, to the market, to the media and to customers. It is particularly important to engage early with regulators, even if it’s just to say “we haven’t got to the bottom of the problem yet but we’re taking it seriously”.

**Ratley:** Some the most important steps that an organisation can take to manage and mitigate the damaging effects of a cybersecurity breach include conducting an investigation to determine the cause of the breach and what information has been compromised, researching applicable breach notification laws that require notice to individuals whose sensitive information has been compromised, providing open and sincere communications to advise affected parties about the breach, supplying honest and timely responses to questions about the breach, and taking steps to remediate the breach and prevent future incidents.

**Zimiles:** This depends on the nature of the security incident that has been experienced. First, we recommend identifying the impacted servers/computers and taking them off line. This means that they will remain powered on but disconnected from the internet/network. Second, if there is malicious data traffic and the ports through which the traffic goes are known or the IP address to which traffic is coming from, block the applicable ports and IP addresses at the firewall if practical. Third, preserve the needed data. These three items are part of the foundation for an effective investigation and response.

**10. How can understanding the different types of cyber-criminal profiles and motives help to identify which resources and assets need the most protection, and how to effectively protect them?**

**Mackenzie:** The motives and perpetrators are many and varied and thus understanding your own business and its risk management framework is often easier to grapple with rather than concentrating on understanding the potential perpetrators.

**AIG’s experience is that losses are often due to staff error or rogue employees, but there is a growing concern that criminals are exploiting businesses’ reliance upon technology.**

Businesses should be across the latest threats and attacks that are occurring, and we find educating employees can be a key differentiator in risk management. An understanding of breaches that have occurred within the organisation’s industry is a good way of monitoring the important assets that may be vulnerable and to provide concrete examples when reviewing the organisation’s risk management framework.

**Zimiles:** Understanding the different profiles and motives of cyber criminals is critical. As they have historically, means and opportunity will continue to drive how fraud schemes and other financial crimes are devised as the criminals will continue to seek, identify and exploit vulnerabilities in any organisation’s controls. This will require companies to continually assess and update both the external and internal risks they are faced with, and will probably to need to conduct those assessments and updates on a more frequent and diligent basis. They will need to monitor and collect key intelligence regarding to crime trends specific to their own industry, operational geographies and third party relationships and leverage that information to enhance and tighten controls as necessary.