VIRTUAL ROUND TABLE

CorporateLiveWire

Fraud & White Collar Crime 2014

MEET THE EXPERTS

James Ratley - Association of Certified Fraud Examiners
T: +44 (0) 207 692 1888
E: jratley@acfe.com

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.

Ben Rose - Hickman & Rose
T: +44 (0) 207 702 5333
E: brose@hickmanandrose.co.uk

Ben Rose leads the corporate crime team at Hickman & Rose. He has immense experience in fraud and white collar crime, including the SFO's first ever proposed international bribery case against EFT Ltd. He acted for directors of Balfour Beatty PLC and Macmillan Publishing and for a senior AON manager in the SFO and FSA corruption inquiries. He represents several LIBOR clients and acts for an Autonomy director in the Hewlett Packard investigation. He advised News Corporation during the Metropolitan Police investigation. He serves on the Law Society's Anti-Money Laundering Panel and is an officer of the International Bar Association.

Satnam Tumani - Kirkland & Ellis International LLP
E: satnam.tumani@kirkland.com

Satnam Tumani is a litigation and regulatory partner in the London office of Kirkland & Ellis International LLP. His practice focuses on a range of white collar and corporate crime matters. Satnam has been appointed to the Law Society's Money Laundering Taskforce. He is a member of the City of London Law Society's Corporate Crime & Corruption committee and is on the Lexis Nexis editorial board for corporate crime. Prior to joining Kirkland, Satnam spent 17 years at the UK Serious Fraud Office (SFO), where he served as head of the Bribery & Corruption & International Assistance divisions.

Steven Molo - MoloLamken LLP
T: +1 212 607 8170
E: smolo@mololamken.com

Steven Molo maintains an active trial and appellate practice representing corporations, boards of directors, funds, special committees, and individuals in complex business litigation, regulatory matters, and white collar criminal matters throughout the United States and abroad. He began his career as a prosecutor in Chicago, he then practiced with Winston & Strawn for 18 years where he was a senior litigator and member of that firm's Executive Committee, he then spent five and a half years as a litigation partner with the Wall Street firm Shearman & Sterling.

He has been recognized by peer and client review for inclusion in Best Lawyers in America (New York: commercial litigation, white collar defense, appeals), Chambers Guide to the World's Leading Business Lawyers, Superlawyers, PLC Which Lawyer? (highly recommended, New York, disputes), Euromoney's Guide to the World's Leading White Collar Crime Lawyers, Leading Attorneys (business litigation, white collar criminal defense, antitrust, appeals), Benchmark Litigation (Circuit Star), Who's Who in America, Who's Who in the Law, and Who's Who in Business and Finance. For the past three years he has been named byLawdragon to its list of 500 Leading Lawyers in America.

MEET THE EXPERTS

Randy Wilson - RGL Forensics
T: +1 636 537 5589
E: rwilson@rgl.com

Randy Wilson takes being a strategic partner for his clients seriously. Clients rely on him to provide sound judgment and expert advice in a variety of situations to solve financial problems.
Working with insurance companies and lawyers, Randy accurately, effectively and efficiently measures losses related to:

- Fraud and fidelity
- Business interruption
- Property loss
- Employee dishonesty and theft
- Marine losses
- Subrogation

Randy's more than 25 year career has covered claims and cases across a variety of industries, including manufacturing, hospitality, retail and consumer goods, ocean marine, professional services, and energy. He has a detailed understanding of the business issues related to franchise ownership and the ocean marine industry, including the unique issues related to government contracting.
A globally recognized financial forensic expert and certified fraud examiner, Randy has been featured in international publications and major media outlets including NBC News and Financier Worldwide. Randy quantifies losses, traces assets and identifies financial motive for fraud schemes ranging from arson and embezzlement to misappropriation and theft. He helps companies detect and prevent theft or fraud, and works with insurance companies on fraud and fidelity claims.

Randy leads the firm's St Louis office. He serves on the board of the Walker Scottish Rite Clinic for Childhood Language Disorders and is an adjunct professor at Webster University where he teaches on special topics in forensic accounting for litigation.

Colleen Conry - Ropes & Gray LLP
T: +1 202 508 4834
E: colleen.conry@ropesgray.com

Colleen Conry, co-leader of the government enforcement practice group at Ropes & Gray LLP in Washington, D.C., focuses on white collar criminal defense and complex civil litigation. She has extensive experience in representing multinational corporations and their executives in government investigations of potential violations of the Foreign Corrupt Practices Act, Food Drug and Cosmetic Act, and securities fraud statutes.

Prior to joining Ropes & Gray, Colleen served as a Senior Litigation Counsel in the Fraud Section of the Criminal Division in the U. S. Department of Justice. In 2007, Colleen received the Attorney General's Award for Distinguished Service and the FBI's Annual Award for Outstanding Criminal Investigation.

Benno Schwarz - Gibson, Dunn & Crutcher LLP
E: bschwarz@gibsondunn.com

Benno Schwarz is one of the leaders of Gibson Dunn and Crutcher LLP's European White Collar Defence and Investigations Practice Group Team. He has long-standing experience advising on compliance matters under the German law, the Foreign Corrupt Practices Act (FCPA), as well as under the UK Bribery Act. A special focus of Benno Schwarz' practice is on the advising in the connection with Compliance Monitorships and investigations in Germany and countries formerly belonging to the Soviet Union, notably Russia.

MEET THE EXPERTS

Sharon van Rooyen - Ernst & Young
E: sharon.vanrooyen@za.ey.com

Sharon van Rooyen is a Partner within Ernst & Young in the Fraud Investigations & Dispute Services practice, focusing on fraud & corruption investigations, fraud risk management and anti-corruption compliance. Sharon holds BCom, LLB, LLM and ACII qualifications. She is an admitted advocate of the High Court of SA, member of the ACFE (International), Director of the ACFE SA Chapter and member of the ICFP.

She is an experienced investigator in the forensic field and has been involved in a number of investigations, both locally and internationally. In the past 17 years she has led a number of assignments in the area of forensic investigations and fraud risk management and anti-corruption compliance.

In addition she has provided training, facilitated workshops and presented on the subjects of fraud and corruption risk management, forensic investigations and anti bribery legislation.

Sharon has vast experience in anti-fraud and bribery consulting, as well as labour law. She has conducted forensic investigations, anti-fraud risk management and anti-corruption compliance reviews in or on behalf of clients in various industries.

Gonenc Gurkaynak - ELIG Attorneys-at-Law
T: +90 212 327 17 24
E: gonenc.gurkaynak@elig.com

Gönenç Gürkaynak holds an L.L.B. degree from Ankara University Law School (1997), and an L.L.M. degree from Harvard Law School (2001). He is a qualified attorney of the Istanbul Bar (1998) and the New York Bar (2002), and he is also a Solicitor of the Law Society of England & Wales (2004). He lectures at three universities in Istanbul and also holds a permanent teaching position at undergraduate and graduate levels at the Bilkent University Law School in Ankara, where he has been teaching since 2004. Gönenç Gürkaynak is one of the founding partners of ELIG, Attorneys-at-Law in Istanbul, and he heads the Regulatory & Compliance Department at ELIG. He has had over 100 international and local articles published in English and in Turkish on various matters of Turkish law, and two books taught at law schools.

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

David Corker has a formidable reputation as a criminal and regulatory litigator. He is ranked as a key individual (Band 1) in the fields of Criminal Fraud and Crime and Cartel Defence by Chambers 2014, and as a leading individual for Fraud by Legal 500 2013 2.

David specialises in acting for clients implicated in criminal or regulatory investigations, many of them international. He has many years' experience of fraud, corruption cases and cartel investigations and also maintains a thriving general criminal practice.

David has acted for clients in almost every large criminal fraud case undertaken by the Serious Fraud Office. He has considerable experience in international criminal cases involving, for example, allegations of corruption, money laundering or cartels. In relation to Financial Conduct Authority investigations, his work has focused on alleged insider dealing, boiler room frauds and misleading the market.

MEET THE EXPERTS

Martijn Hin - BDO
T: +31 (0)30 284 9715
E: martijn.hin@bdo.nl

Martijn Hin is a chartered accountant and leads the Forensics & Litigation Support practice at BDO Netherlands, specializing in forensic investigations and litigation support, including forensic IT solutions.

Responsible for establishing BDO's Forensics & Litigation Support practice in the Netherlands, Martijn has significant experience in providing forensic accounting services as related to cross-border investigations. He has directed matters involving allegations of earnings management, potential violations of Anti bribery and corruption regulation (like the Foreign Corrupt Practices Act (FCPA) and UK Bribery Act), disputes in both civil and criminal matters, as well as investigations involving various types of general fraud and misconduct issues.

John P. Rupp - August & Debouzy
E: jrupp@augdeb.com

John P. Rupp is a partner in the London office of Covington & Burling LLP and specializes in handling bribery and other corruption related issues. His work has included designing compliance programs and investigating possible wrongdoing. Before relocating to Europe in 1995, Mr. Rupp practiced for more than 20 years in the Washington office of Covington & Burling. He also has spent time in the Solicitor General's Office at the US Department of Justice. In addition to publishing many articles on corporate compliance issues, Mr. Rupp has taught courses on corporate compliance at American University, Georgetown University, University of Iowa and the Ecole de Formation Professionnelle des Barreaux de la Court D'Appel de Paris. Mr. Rupp graduated from the Yale Law School in 1971.

Fraud & White Collar Crime 2014

The Fraud & White Collar Crime landscape has changed - and continues to change - significantly, particularly in the aftermath of the Libor scandal. We spoke with 12 experts from around the world to discuss recent regulatory changes and interesting developments, outline how an organisation can safeguard against fraud and white collar crime and share their opinions on the biggest cases and trends to look out for in 2014.

1. White collar crime remains a priority for many authorities. What crimes are occurring most frequently in your jurisdiction?

Ratley: Asset misappropriation is still the most common type of occupational fraud, and within that rather large category are a few types of crime that occur more frequently than others. In the ACFE's 2012 Report to the Nations on Occupational Fraud and Abuse, we found that fraudulent billing schemes were present in nearly 25 per cent of fraud cases, followed by non-cash misappropriations (such as stealing inventory from a warehouse) at 17 per cent, and expense reimbursements and skimming, both at 15 per cent. In general, wherever there are employees with access to a company's assets and the opportunity steal, there is a heightened risk of fraud. Not all employees are dishonest, of course, but it only takes one to have an impact on your bottom line.

Rooyen: In the recent past we have noted that the prevalence of economic crime differs from region to region in our area of operations. One would for instance find that while tender fraud in the construction industry, is prevalent in the Limpopo province of South Africa, fraud in the public sector is prevalent in Kwazulu Natal province and facilitation payments and inappropriate gifts common in for instance, Nigeria.
In general it would however appear that the majority of economic crime perpetrated in our jurisdiction is in some way related to the procurement of goods and/or services and often involves some form of collusion or corrupt relationship.

Schwarz: In terms of the sheer volume of fines (not the number of violations), antitrust and tax violations, violations of trade sanction regimes and anti-corruption laws have been on the top of the agenda. However, the volume is not reflective of the frequency in which these violations occur, but the money volumes involved with the issues at stake. In terms of frequency of violations, crimes related to fraud represent still the largest group followed by data theft and violation of IP rights. My guess would be that violations in the field of data privacy will be on the top of the list in the years to come. At least the respective laws leading to higher fines and criminalising unwanted conduct are in the making already.

Tumani: The UK National Fraud Authority ("NFA") conducts an annual fraud measurement exercise, named the Annual Fraud Indicator. The latest Annual Fraud Indicator estimates the total cost to the UK from Fraud as £52 billion. Fraud against the private and public sectors is estimated at £15.9 and £20.6 billion respectively, whilst the cost to UK individuals is £9.1 billion. The analysis identifies identity fraud and cyber enabled fraud as particularly significant which is perhaps unsurprising given the increased use of the internet in most forms of interaction with commerce and the government. I would expect this trend to continue and it is notable that both the public and private sectors have repeatedly identified cyber-crime as a major threat.

Wilson: According to its 2012 biennial Report to the Nations survey of actual cases, the Association of Certified Fraud Examiners (ACFE) reports that the most common type of fraud schemes in the study included billing fraud followed by corruption, expense reimbursement, and skimming. Other schemes making the top 10 included cash larceny, check tampering, payroll and financial statement fraud.

The United States Securities and Exchange Commission (SEC) recently published the incidence of its enforcement actions for the 10 years ended 2012. The categories portrayed in these statistics provide insight into the incidence of fraud. In the most recent three years of these statistics, these categories include increases in actions against investment advisers, investment companies, broker-dealers and to a lesser extent but significant, securities offerings. Obviously these are in response to the mega-Ponzi era in the United States that began with the discovery of Madoff's massive fraud in 2008.

Gurkaynak: The white collar crime that is most frequently investigated and therefore that occurs most frequently is bribery, followed by bid rigging, malversation and

malfeasance. Putting aside the most recent corruption investigation - which included the sons of three cabinet ministers, the general manager of state-owned Halkbank, a business tycoon and the Mayor of the Fatih Municipality (a regional municipality in Istanbul) - the enforcement of anti-corruption laws mostly concentrates on municipalities. Just last month, a bribery case against the members of the Kayseri municipality was resolved in a first degree court with two people being sentenced to approximately seven years of imprisonment due to bribery and malversation.

Rupp: The number and variety of prosecutions for white collar crime have been increasing dramatically over recent years. They have also been increasing when viewed from a geographic perspective, in part because of a growing realisation among prosecutors that putting individuals in jail has more deterrent value than a company prosecution. The surge in prosecutions for white collar crime – commercial and public bribery, insider trading, price fixing, embezzlement, money laundering, trade sanction violations, health and safety offenses, failing to report adverse drug effects – shows no sign of abating. I personally spend a good deal of time on bribery and money laundering cases, which tend to cut across national boundaries. The upward trend in that area has been unmistakable, with one priority criterion – long custodial sentences – no longer being exceptional at all.

Hin: Due to the financial crisis, companies' profit margins are under pressure. Therefore, firms are reviewing their financial results in more depth. This induces more identified cases of white collar crime. In at least 60 per cent of fraud cases, the organisation's employees are involved. Financial statement fraud and the misappropriation of assets are the most prevalent frauds. Financial statement fraud by management is often motivated by increased pressure to improve a company's financial performance. Also a fraudster might rationalise his unethical behaviour based on a change in the work climate arising as a consequence of the financial crisis. Based on our experience the absence of bonuses and increased working pressure are important factors.

Rose: Financial crime remains high on the law enforcement agenda. There has been a recent and noticeable increase in financial regulatory prosecutions against both individuals. Many of these actions relate to the Libor/Eurobor and foreign exchange investigations. Simultaneously there are enforcement proceedings concerning inadequate systems and controls, failure to discharge statutory responsibilities, false accounting, disclosure offences and insider trading.

Cross-border bribery and corruption investigations and prosecution are also increasing. These often arise out of mining or infrastructure activities in emerging markets, where companies have had historically lax controls and work overseas.

Finally, the political turmoil in the Arab world has led to companies and individuals facing prosecutions for breaches of sanctions laws.

Despite the widely recognised gold standard established by Bribery Act the SFO's ability to deliver following the debacle of the Tchenguiz and Dahdaleh cases is now in serious doubt

Molo: FCPA, insider trading, securities fraud, public corruption, tax fraud, and antitrust continue to be priorities of federal prosecutors in New York, as well as other jurisdictions in the United States.

2. Following the Libor scandal we have witnessed a trend for increased financial penalties and forfeitures imposed on large organisations (such as GlaxoSmithKline and BP's Deepwater Horizon). Are you concerned that this could set a dangerous precedence?

Corker: The fines against banks and institutions for failure to prevent wrongful conduct, as in for example the Libor scandal, are rapidly escalating and it appears that the mindset of the FCA has been that deterrents and justice require hugely increased financial sanctions.

Schwarz: For Germany, there is definitely a noticeable trend to increase fines. Only last year the German legislature has introduced significant amendments to the German Administrative Offences Act (OWiG) that are testament to this, namely the tenfold increase of corporate fines for offences committed by bodies or executives of corporations in violation of legal duties affecting the corporation, or for the failure to establish effective controls to prevent law violations, to up to EUR 10 million for intentional conduct, and up to €5 million for negligent conduct, respectively. Further, it is worth noting that the

aforementioned maximum fines can be exceeded without limitation up to the benefits the corporation derived from the misconduct, e.g. including profits made under a contract that was illegally obtained by bribery. Such indirect disgorgement of profits may easily exceed the mere administrative fine amount by multiple times. Additional change on the horizon is the plan to introduce a criminal code for enterprises, which would further increase the ability to fine corporations and drive up the amount of fines.

Tumani: Corporates are exposed to criminal and regulatory consequences more than ever before. The public interest in matters relating to corporate crime is high. The Financial Conduct Authority ("FCA") imposes fines that will act to disgorge benefits, to discipline offenders and to send a deterrent message to the market. The UK Sentencing Council has issued a consultation in respect of a proposed new and tougher approach to fines for corporate criminal offending. It must always be remembered however that the punishment of a corporate will have potential collateral consequences for associated innocent parties, whether they be pension funds, employees or suppliers. Systems of punishment must therefore have regard to the overall fairness of the penalty in any given case.

Rupp: There is a risk of one-upmanship so far as financial penalties are concerned, with prosecutors competing with one another for verdicts with eye-popping penalty numbers. At the same time, however, corporate executives need to understand that prosecutors and courts in country after county are more sensitive now than they ever have been to the damage that white collar crimes often involve. The Libor scandal is one example of that. Even more fundamentally, many people have concluded – rightly or wrongly – that the recent financial meltdown was caused in large part by malfeasance among white collar actors. Seeing people in India and many other countries taking to the streets to protest bribery and other forms of corruption should prompt a full reconsideration in the boardroom and among senior executives of whether paying bribes to obtain or retain business, to take one further example, is a smart way to do business.

Hin: The financial economic crisis has made stronger international supervision of financial institutions and the financial system necessary. Currently the European Union is establishing European supervision of the financial markets through, for example, the European Banking Authority (EBA) and the European and Securities Market Authority (ESMA). European regulation is harmonised with current international standards from the US and UK. With respect to bribery and corruption we have observed a significant increase in the number of investigations of Dutch companies carried out by supervisory authorities in the US and UK. We expect that foreign supervisors will further extend their focus to multinational financial and non-financial organisations and that the increased activity of European supervisory authorities will lead to more administrative penalties.

Molo: Dangerous or not, the precedent is there. The public now expects aggressive enforcement and stiff penalties. A more dangerous precedent is those companies throwing executives under the bus in an effort to help themselves. The deferred prosecution agreements through which these financial penalties are imposed incentivise companies to point the finger and assign blame to individuals as a means of "cooperation" intended to lessen the financial blow. As a result, more executives are finding themselves subject to scrutiny by prosecutors that begins with accusations from the company's own lawyers – who are interested primarily in limiting exposure to the company. These incentives for "self-reporting" and "cooperation" are coming under increasing criticism in the United States.

3. With reference to the Libor scandal, how should an organisation safeguard themselves against fraud and white collar crime, and where does the buck lie if they are found guilty?

Corker: In terms of criminal liability the buck must lie with the financial traders if they knew what they were doing, which would be regarded by most people as dishonest. In terms of the management or organisation, there isn't yet an offence in English criminal law of failure to prevent fraud. However the current Director has suggested that there ought to be. In terms of regulatory sanctions which have been applied to all the banks in light of the Libor scandal, it's obviously from the FCA's decision that the level of the fine was increased because of management failures to prevent traders from allegedly manipulating Libor. To protect yourself against such sanctions you need to have effective management and a commitment to confronting

traders' attitudes.

Schwarz: There is a saying that has been true for years, but, sadly so, is still disregarded by many, and therefore merits repeating: One Euro invested in prevention equals 10 Euros spent in dealing with the consequences of white collar crime.

For me, another important lesson learnt from the Libor scandal was to see again that a vigorous and expedient investigation and open and transparent cooperation with the relevant authorities will make a huge difference in the ultimate outcome of the matter and the size of the fine and the ability of the offender to mitigate the consequences of the violation. This is definitely the case for antitrust violations where formal leniency programs exist, but remains also critical for investigations in other focus areas, notably anti-corruption, tax and export sanctions).

Germany, for example, last September has introduced a totally renewed Act on Foreign Trade (Außenwirtschaftsgesetz) that comprehensively regulates the trade sanctions regime and for the first time also provides for a leniency program in that area that may exempt an offender from fines in case of self-disclosure of identified violations to the competent authorities.

Tumani: The law relating to corporate criminal liability is markedly different as between the UK and the US. In the UK a corporate will not generally be guilty of a crime unless it can be shown that the directing mind and will of a company (Directors and in some cases senior managers) were aware of the conduct. Thus where senior individuals are aware of or involved in criminal conduct they will incur personal liability as well as giving rise to corporate liability. There are now specific rules relating to the provision of LIBOR submissions which should be followed alongside the broad principles as to conduct set down by the FCA. These rules require independent verification and audit as a safety measure. Following the furore that accompanied the LIBOR case the Director of the Serious Fraud Office ("SFO") called for a debate on the introduction of a failure to prevent fraud offence modelled on the s7 offence in the UK Bribery Act. It may be that this will find favour in the upcoming legislative timetable. In the meantime corporates looking to prevent fraud could usefully modify and then apply the principles outlined by the Ministry of Justice's guidance on adequate procedures to prevent bribery.

Rupp: Some instances of bribery that we have investigated were demonstrably the result of misconduct by a rogue employee. More often, however, the fault can be traced to the company's failure to provide the needed context – or incentives – for a zero tolerance policy for non-compliant conduct. The Libor scandal is a good example. The Libor scandal did not spring from the mind or confirm the inclinations of a single individual. The Libor scandal involved widespread misconduct among the employees of numerous entities. When a Libor-type scandal emerges, one has to ask whether there was an appropriate "tone from the top," whether the prevailing incentives within the organisation were supportive of or were at war with compliance, whether the compliance function within the organisation was properly resourced. I'm not going to express an opinion on those and other issues with respect to any single organisation implicated in the Libor scandal. But those and other similar questions need to be considered repeatedly within organisations that want to avoid being on the wrong end of a Libor-type scandal.

Hin: Organisations should implement adequate measures to prevent fraud and white collar crime. When designing and implementing controls, we advise companies to pay special attention to striking a balance between hard controls such as procedures and rules and soft controls such as culture, leadership and integrity. The effectiveness of hard controls within organisations depends on the presence and operation of soft controls and the characteristics of individual employees. It is a challenge for firms to identify existing soft controls and to adjust them accordingly to achieve the desired effect. The consequences of corruption can be enormous. Reputational damage can cause great damages, and directors can be held personally liable for example if the organisation did not implement adequate measures to prevent bribery and corruption. In general is an adequate risk control framework helping to minimise the penalties to be paid to the controlling authorities.

Conry: The Libor scandal indicates that transnational investigations are on the rise. In this global enforcement environment, multi-national corporations are subject to scrutiny of both their domestic and their international operations. Moreover, governments are demonstrating an

increasing willingness to hold entities criminally responsible for the conduct of individuals—including mid-level employees. As a result, corporations need compliance programs that are robust globally. Specifically, this means that companies should (1) have policies containing clear rules and that provide guidance about the exercise of discretion; (2) implement effective training on regulatory requirements; (3) tightly monitor employee conduct, including all modes of communication relevant to that business (such as Bloomberg chats); and (4) respond appropriately to any red flags.

Molo: Vigorous compliance efforts, of course, serve the purpose of deterring misconduct and also demonstrating to authorities that the company is serious about following the law. The buck is less and less likely to stop with mid-level manager. The exposure companies face when subject to serious investigations – financial, reputational – is huge. Investigations can absorb a great deal of senior management time and can present a major distraction from the company going about its business. They also can damage employee morale and hurt recruitment and retention efforts. As a result, shareholders, and the public generally, are demanding accountability. And prosecutors are becoming more aggressive in holding those at the top responsible. Look for more prosecution forays into the C-Suite.

4. As Ralph Lauren have recently discovered, multi-national organisations are not exempt from facing corruption allegations on more than one front. How can you assist an organisation facing successive prosecutions in multiple jurisdictions arising out of the same factual basis?

Rooyen: Many African countries already have robust anti-bribery and corruption (ABAC) legislation, a number of which include extra-territorial reach and ban facilitation payments. Additionally, in the last few years we have started to see African regulators commencing derivative actions against companies already under investigation by US prosecutors for alleged FCPA violations.

As is true in so many aspects of life, prevention is better than cure. Many of these risks can be missed without awareness, careful due diligence and oversight. Rigorous fraud and corruption risk assessments should be conducted and revisited regularly. Policies and procedures to mitigate these risks should be tailored to the specific business and geography, and supported with adequate local language training.

Schwarz: Within the EU there are regulations, albeit vague, preventing double-jeopardy. It is more difficult in the context between Europe and the U.S. and even more so in the relation jurisdictions that are less integrated with our market economies, such as China or Russia. In these cases a lot hinges on the ability of the company and its advisers to create trust with all involved authorities and provide for a roadmap that helps the different regulators to come to a reasonable outcome in the various jurisdictions. Unfortunately, recent examples – even between Germany and the U.S. – show that this can be challenging. Germany has a federal system whereby prosecutor's offices are less coordinated than you would wish in these complicated cases, and the individual handling preferences of a single prosecutor can drive the agenda in very substantial matters. Not ideal, but this is the world we are operating in.

Tumani: Traditional approaches to jurisdiction were largely focussed on activity within the confines of each country's own borders. In the field of corruption, the origins of multi-jurisdictional casework come from the OECD convention which requires countries to assert jurisdiction over the activities of their nationals and companies abroad. The LIBOR cases also demonstrate that companies which operate across boundaries risk exposure to multiple enforcement agencies. In order to manage exposure it is essential to seek engagement with the relevant national regulator. Once engaged the lead regulator will manage the extent to which other countries become involved in a case. In international cases the Eurojust guidelines and the protocol between the respective Attorneys General of the UK and the US set down a framework for countries to manage and, in appropriate cases, limit multi country investigations. Absent early engagement, prosecuting departments will invariably send mutual legal assistance requests abroad and will thereby expose a company under investigation to multiple foreign regulators.

Rupp: Putting aside for the moment whether Ralph Lauren should have been prosecuted for bribery despite the robustness of its anti-bribery program, there is a premium on considering early and often as pertinent evidence is collected which countries may be able

to assert jurisdiction over the particular matter and then developing a strategy designed to avoid multiple – or, even worse, successive – prosecutions for the same conduct. Understanding prosecutorial inclinations in many countries tends to be of key importance in that connection. One also has to understand when and where the reporting of non-compliant conduct is required under either applicable bribery or money laundering statutes. The risk of multiple prosecutions for the same conduct generally can be managed with appropriate foresight and knowledge.

Hin: In this situation we do cooperate with law firms to perform cross-border engagements. As an independent forensic accountant we perform investigative procedures to report the relevant facts and circumstances. The scope of our work is in alignment with the requirements from a law perspective per jurisdiction. These kinds of engagements are performed under legal privilege. The law firm uses our report(s) in their defence strategy in the multiple multi jurisdictions.

Conry: The United States and United Kingdom have traditionally led the way in prosecuting corruption. However, other countries that have been historically less active in this area have established new enforcement tools or legislation recently. For example, Russia passed two key pieces of anti-corruption legislation last year, a new anti-corruption law became effective in January 2014 in Brazil, and Chinese President Xi Jinping has stepped up enforcement and investigation through his "tigers and flies" campaign. Given this context, companies must be aware that they can be subject to liability in multiple jurisdictions. Corporations can best protect themselves by creating an anti-bribery policy that is in line with the statutory requirements in the most stringent jurisdictions (i.e., the U.S. Foreign Corrupt Practices Act and the UK Bribery Act). In addition, many anti-corruption laws provide that self-disclosure can help mitigate penalties. If companies discover an issue in one country, they should consider proactively investigating the conduct in other countries and disclosing to the relevant entities. Companies can also request to consolidate investigations in multiple jurisdictions into one global resolution.

Molo: It is best to try to get out front if you believe there is a realistic chance of multi-jurisdictional enforcement. You must assume that representations, disclosures, or admissions made in one jurisdiction will be accessible to authorities in another jurisdiction. Greater and greater coordination among countries is the norm. It is important to have a core team coordinating efforts across the board, with experienced, well-regarded specialists in each jurisdiction in which investigations have begun or are likely to commence. The core team should solicit the views of the counsel in the various countries to assess the relative risks and benefits of key steps along the way.

5. Have there been any recent regulatory changes or interesting developments that could yet shake up the litigatory landscape further?

Corker: The SFO are looking for a first prosecution against an organisation under Section 7 of the Bribery Act 2010, i.e. failure to have in place systems and controls to prevent bribery by one of its employees or agents. The Libor prosecution will obviously be a headline case. The FCA's ever increasing commitment to prosecute financial crime such as insider dealing, acting whilst unauthorised, etc.

Rooyen: Corruption continues to be pervasive around the world. Increased enforcement by international enforcement agencies has left multinational organisations vulnerable to international corruption investigations and significant financial penalties and even jail sentences for its employees in instances where they are found guilty of corruption.

South Africa has its own corruption legislation, the Prevention and Combating of Corrupt Activities Act ("PRECCA") which makes it a crime to offer or receive a bribe, both in the public and private sector.

Although the enforcement of PRECCA has not been as widespread as the enforcement of the Foreign Corrupt Practices Act ("FCPA"), in the United States and the UK Bribery Act in the United Kingdom, we expect the enforcement of PRECCA to rise. Our expectation is based on the active enforcement culture of international enforcement agencies and the fact that the South African Companies Act of 2008 now includes regulations requiring companies to comply with the recommendations of the Organisation for Economic Co-Operation and Development's Anti-Bribery ("OECD") Convention.
Furthermore many countries in Africa, such as for instance Namibia, Botswana, Nigeria and Kenya have Anti-Bribery

and Corruption legislation, many with extra territorial jurisdiction, which is expected to further strengthen the active enforcement culture.

Schwarz: A more fundamental development to watch out for in Germany is the proposed adoption of a "Corporate Criminal Code" (Verbandsstrafgesetzbuch), under which - for the first time under German laws - criminal sanctions could be imposed directly against corporations. On 14 November 2013, a majority of the justice ministers of the German states resolved to introduce a bill for such a Corporate Criminal Code into the legislative process.

The draft bill includes profoundly aggravated liability exposure for corporations facing criminal investigations and sanctions. This includes a legal obligation of prosecutors to open investigations into allegations of corporate misconduct, limiting currently existing discretionary powers. Further, the range of possible sanctions against corporations would be widened not only to include monetary fines, but also warnings with suspended sentences, the publication of criminal convictions, a debarment from public subsidies or public tenders, and, as a last resort, the compulsory liquidation of the corporation.

On the positive side, the draft bill acknowledges an effective compliance system for the first time as a defence against or a mitigating factor to reduce fines. This is an interesting development to watch out for in the next year.

Tumani: The last year has seen a raft of changes in the field of economic crime and regulation. The UK's principal competition agencies (the Competition Commission and the Office of Fair Trading) have been merged to create a unified Competitions & Markets Authority. There have also been changes to the criminal cartel offence. The requirement to show dishonesty has been removed and the new offence appears to be significantly easier to prove. The last year has also seen a more muscular approach to professional regulation. For example the Accountancy Regulator has concluded a significant case with record fines against firms and members of the profession involved in the affairs of MG Rover. Finally the SFO will soon have the ability, in appropriate cases, to seek a deferred prosecution agreement ("DPA") with a company under investigation.

Wilson: Probably the most recent such development was the announcement during the summer of 2013 by the SEC regarding the establishment three new initiatives that focus on detecting fraudulent conduct. These include the Financial Reporting and Audit Task Force, the Microcap Fraud Task Force and the Centre for Risk and Quantitative Analytics. It is quite clear from the announcement that the SEC is stepping up its efforts to detect fraudulent financial reporting as well as abusive trading and fraudulent conduct in securities. The SEC is also ramping up its continuing use of technology including forensic data analytics with establishment of the new Centre for Risk and Quantitative Analytics.

The Dodd-Frank Act also continues to dominate the landscape of regulatory changes in the United States in that it provides the SEC with the authority to reward tipsters whose information leads to significant monetary sanctions against entities and individuals committing such frauds.

Gurkaynak: Recently, the parliament has amended the Judicial Police Regulation to provide that all investigations realised by the police with the instructions of public prosecutors should be notified to the highest ranking local administrative authority such as the governor, which would indirectly lead to the investigations conducted by the police to be reported to the Ministry of Internal Affairs. However, the High State Court has suspended the execution of the relevant amendment.

Aside from the aforementioned, another significant change in the Turkish legal landscape was the enactment during 2013 of the Law on the Prevention of Financing of Terrorism numbered 6415 and its corresponding Regulation, which are mainly concerned with the freezing of assets of the persons listed in certain UN Security Council decisions.

With regard to bribery laws, the latest amendment was realised on July 2012 with the criminalisation of private-to-private bribery and the broadening of the scope of both domestic and foreign bribery.

Rupp: We have been distributing on almost a monthly basis reports to clients on recent developments relating to bribery and money laundering as well as other compliance issues. On bribery and money laundering, we have seen during the past year or so potential watershed developments in multiple countries, including Brazil, China and Russia – all of which recently

have adopted new statutes dealing with the bribery of foreign government officials. And even when a country has not changed its legislation, one needs to keep an ear to the ground for important prosecutorial policy changes. Not too many years ago the general thinking among anti-bribery experts is that there was little risk of prosecution in China for bribery by or on behalf of a multi-national company, with the consensus being that the Chinese authorities were anxious to avoid deterring foreign investment by taking an aggressive posture on bribery. Those days are well and truly past.

Hin: The impact of international investigations carried out by supervisory authorities is being underestimated by Dutch companies. Most Dutch organisations do not realise they are susceptible to international scrutiny, nor do they fully comprehend the size of the potential fines they will face for non-compliance with regulations. For example Dutch organisations often have transactions with foreign UK or US organisations but are mostly not aware of the UK Bribery Act and the US Foreign Corrupt Practices Act (FCPA) are applicable to them. When possible future pressure or even penalties are being applied from these laws, Dutch organisations will probably pay more attention to the preventive guiding procedures concerning these laws. We suspect the increased international focus of supervisory authorities will result in Dutch and European regulations being brought more and more in line with those from the US and UK.

Rose: The most important change coming to the United Kingdom is the introduction of deferred prosecution agreements ("DPA"). These allow companies to conclude criminal investigations by providing a series of undertakings including compliance inspection and monitoring. Subject to the on the appetite of the SFO and the attitude of the Courts these may well fundamentally change fundamentally the relationship between prosecutors and corporate entities. Assuming they take off the prospect for individual suspects, who fall outside of this new regime, is pretty gloomy.

Conry: For the last 40 years, the SEC has permitted defendants to settle enforcement actions while neither admitting nor denying the underlying allegations. In June 2013, the SEC announced that it would begin requiring admissions in certain serious cases involving harm to large numbers of investors, egregious intentional misconduct, or obstruction of an SEC investigation. This policy change has important implications, because admissions in an SEC settlement may be used in parallel private litigation. It is unclear how often the SEC will in fact insist on such admissions – the June 2013 announcement stated that most cases would still be resolved on a no-admit, no-deny basis. If the SEC takes a hard line on this policy, however, defendants may choose to litigate more securities matters, rather than settle them.

Molo: There is a clear focus on coordinated anti-corruption enforcement around the globe. The U.S., under the FCPA, and the U.K., under the Bribery Act 2010, are at the forefront but hardly alone. Many other countries are engaged. Last year, Brazil enacted its Anti-corruption Bill of Law, or "clean company law," to much fanfare. The year prior, Mexico enacted its Federal Law Against Corruption in Public Procurement. Look for similar new laws in developing countries around the world. While it would be nice to think that this new legislation emanates from a belief that corruption is simply wrong and extracts a high and unfair societal price, in reality these countries are realising that enacting and enforcing anti-corruption laws is a requirement to participate in international trade at its highest level. The Organization for Economic Cooperation and Development has exerted substantial influence to affect change.

6. In your opinion, what are the biggest and most interesting cases to follow in 2014?

Ratley: While it is not a single case (but more of an evolving issue), I think the response from governments, businesses and anti-fraud professionals on how to deal with Bitcoin will be one of the most interesting stories this year. This virtual currency has been gaining in popularity around the world. While it is used by many as a legitimate currency, it has also been involved in Ponzi schemes, money laundering and other financial crimes. Anti-fraud professionals are catching on: learning how to track illegal transactions, along with using undercover operations and other methods, will be paramount in countering Bitcoin fraud.

Schwarz: There are a number of interesting tax cases that are pending in the financial sector, notably the tax treatment in Germany of so called cum-ex – transactions and cases stemming

from recent enforcement actions to break up merry-go-round-schemes in the VAT area. From the recent media coverage it appears that there will be more light shadowed on a number of large transactions in the defence sector (notably in Greece), which may trigger interesting follow-on cases against German companies. Finally, a few trade sanction cases have been initiated last year against various German financial institutions, which will get into a more advanced stage in this year and will provide additional guidance how these matters are handled by the enforcement authorities and courts in the context of a large scale matter. There are a lot of interesting things to watch out for in Germany, against the backdrop of an increasingly sensitive public audience and legislator.

Tumani: The SFO is bringing criminal proceedings against two companies, Olympus Corporation and its UK subsidiary Gyrus Group Limited. Olympus and a number of its executives have been prosecuted in Japan. The UK allegations relate to a number of Companies Act offences. The case arises out of the referral made by the former CEO of Olympus, Michael Woodford, a high profile whistleblower. The SFO has also brought proceedings against a number of individuals in the Libor cases which will go to trial next year alongside the SFO's first prosecution of individuals under the UK Bribery Act (a case relating to Sustainable AgroEnergy Plc). Meanwhile the FCA has launched an investigation, alongside several other agencies, into a number of firms trading the foreign exchange market. The investigation is at an early stage and it will be some time before the FCA is able to conclude whether there has been any misconduct but nevertheless developments will be closely watched.

Gurkaynak: By far the most interesting case to follow in 2014 will be the on-going investigation that contains allegations with regard to money laundering, bribery and gold smuggling made against the sons of three cabinet ministers, along with the general manager of state-owned Halkbank, a business tycoon known for gold trade and several other businesspeople working in the construction sector. Subsequently three cabinet ministers have resigned in face of the allegations, which have also led the Prime Minister to reshuffle the cabinet.

In addition to the above, several officials of the İzmir Port Administration and several businesspeople have been detained in January 2014 as part of another investigation entangled with allegations of bribery, malversation and bid-rigging. Even though the prosecutor who was administering the investigation has been reappointed, this case too will be on our watch list in 2014.

Rupp: In the bribery area, the Walmart investigation/prosecution has to be watched closely. So, too, does the GlaxoSmithKline investigation/prosecution in China. There also are many individual prosecutions that are likely to resolve, or begin to resolve, issues under the US Foreign Corrupt Practices Act about which reasonable people long have differed, including who qualifies as a "foreign government official," the jurisdictional reach of the US FCPA, in what circumstances an individual can be deemed to have "acquiesced" in non-compliant conduct and thus be vulnerable to prosecution.

Rose: The Libor prosecutions will commence in the first half of this year. Although many of the institutions have already concluded settlements, individuals have yet to have their cases heard. These cases are likely to be the high watermark of the post financial crisis regulatory and law enforcement response.

The investigation into ENRC is one to watch. It will be interesting to observe whether or not the company or any individuals are charged.

The trials of those involved in the alleged "hacking" at News of the World will conclude. Whatever the result, there are lessons to be learned in the areas of ethics, culture compliance, managing investigations and the role of the criminal law and business.

Conry: In the health care context, I will be watching United States ex rel. Nathan v. Takeda Pharmaceuticals NA Inc. In January 2013, the Fourth Circuit issued this opinion affirming the prevailing standard that False Claims Act ("FCA") relators must plead with particularity that a defendant actually presented false claims for payment to the government in order to satisfy Rule 9(b) of the Federal Rules of Civil Procedure. The Supreme Court has accepted cert in this case, to decide whether presentment must be pled with specificity or whether a relator need only plead details of a "scheme to submit false claims" along with "indicia" that false claims were submitted. This case could have important implications for the viability of future whistleblower complaints that speculate about the submission of false claims.

7. What areas of fraud currently provide major organisations with reason for concern?

Ratley: For large corporations, financial statement fraud is always a serious threat. While these cases occur less frequently than other types of fraud, they are by far the most costly. The emphasis placed on share price has been a game-changer for management at many large public companies, who feel increased pressure to meet expectations. This increased pressure can sometimes lead to cases of financial misstatements and fraud just to fulfil these expectations, as opposed to fraud that is perpetrated purely for the fraudster's personal gain.

Schwarz: With the moving of critical transactions into the virtual world of the internet, any kind of cyber-crime will create major challenges for the large and small organisations, and – if not managed prudently – may go to the core of their business model or put them out of business entirely. While most prevention efforts go into the technical side of this issue, an increase international and world-wide cooperation of the enforcement agencies becomes a mission critical to ensure a sustained and secure development of online transactions and avoid online fraud. My concern is that regulators world-wide have not yet delivered many answers to these pending questions.

Tumani: The FCA has been increasingly focussed on the approach of the regulated community to money laundering. They have been critical of the approach taken by banks in respect of Politically Exposed Persons and also focused on the asset management industry's approach to money laundering and bribery and corruption risk. The FCA has made clear that they see this as an area for improvement and we can expect to see more enforcement action in the future. More generally the threat of cybercrime has increasingly focussed the minds of major organisations. A high profile example is the recent case involving Sony. Sony were subject to attack by hackers seeking access to personal details of subscribers to Sony services. As a consequence of this Sony were subject to enforcement action by the Information Commissioners Office in respect of data protection breaches. With changes to data protection laws pending and increased fines for non-compliance this will be an area of concern for many. Finally the SFO has indicated that it has a number of corporate UK Bribery Act cases under investigation. Companies will look closely at the outcomes in these cases so as to be sure that their own approach to anti-corruption is as effective as possible.

Wilson: In my view the areas of fraud that major organisations should be concerned about are financial statement fraud driven by the motivation to achieve otherwise unattainable results including those that drive officer compensation. Aside from the reference to the traditional fraud triangle of motive, opportunity and rationale, the primary reason I believe these organisations should be concerned is that these types of cases tend to be much larger in magnitude than misappropriation and they open the organisation up for enforcement by federal authorities.

These frauds are also more difficult to detect due to the circumvention of controls. According to its report on Fraudulent Financial Reporting from 1998 through 2007, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) pointed out that in cases involving financial statement fraud, the CEO or CFO of the entity was named as being associated with the fraud in 72 per cent and 65 per cent of the cases, respectively.

Gurkaynak: Although Turkey has not witnessed many criminal investigations against legal persons, a few existing cases shed some light onto the areas of concern for companies. The emerging pattern suggests that major organisations should be wary when it comes to crimes of bribery and bid-rigging. By way of example, the highly popular Roche case, which resulted in the acquittal of seven defendants and the non-charging of 11 defendants due to the expiry of the statute of limitations in April 2013, had been initiated due to allegations concerning bid-rigging. In addition, the investigation against 3MTurkeywas also initiated due to allegations of bribery.

Rose: Employee fraud, particularly in accounting functions remains an area of concern. Notwithstanding extensive systems and controls, individuals can often bypass these controls to steal funds, misrepresent accounting reports, improperly use corporate credit accounts and/or cover up historical wrongdoing.

There is heightened focus on tax frauds. Companies are reviewing their tax advice for greater certainty that there is no exposure even to an accusation

of improper tax practices.

Identity fraud is a growing cost to large organisations especially in the financial sector. More sophisticated criminals are using technology to bypass checks or imitate customers.

8. With more high quality data becoming available to fraudsters, how can a company safeguard themselves against the threat of internet or external fraud?

Ratley: The keys to being protected against threats of cybercrime and data breaches are proper employee training and having an expert security team in place to counter those threats. The risks posed by this type of fraud are especially significant among small businesses. As fraud becomes more technologically sophisticated, smaller organisations are often left behind, without the resources or the knowledge base to implement proper data security measures. This leaves them vulnerable to online theft schemes, hacking and malware/viruses that can affect an entire network and seriously impede business operations. It is imperative that anti-fraud professionals working with organisations that conduct business online help them thoroughly assess their security weaknesses and recommend steps to correct them.

Rooyen: According to the 2013 Norton Cybercrime report:
• South Africa is third highest country in the world affected by cybercrime;
• 1 million victims per year; and
• Losses amount to approximately R3.7 billion per year.

As digital information storage continues to transform our working environment, we have found that computer forensic analysis of digital evidence is becoming the norm in most forensic investigations.
Furthermore, protecting a company against unauthorised intrusion and/or external attacks has become imperative. Preventative measures, should as a minimum, include:

• Implement intrusion detection systems
- Identify and protect critical assets;
- Monitor network activities; and
- Supplement firewalls and other forms of network security.

• >Hacker detection methods

- Log management and analysis;
- Data security; and
- Security reviews.

Schwarz: The benefits of the internet in the last decade have been gained on a background of loose regulation, policing and a "wild-west"-spirit of all participants involved. With the maturing of business operations that hinge on the functioning of all processes involved in online businesses a revision of all legal elements involved in a transaction handled through the internet becomes a mission critical. While the front-end of conducting business through the internet has been hugely facilitated, the "back-end" of the processes needs to be tackled to minimise exposure stemming from fraud or other cyber-crimes. This requires a comprehensive analysis of all transaction steps to work on each detail that can create risks or become an entry gate for fraudsters. A herculean task, but unavoidable.

Tumani: The increasing threat posed by cyber-crime has been recognised both within companies, government and anti-fraud agencies. The National Fraud Authority is due to launch a cyber-crime initiative in January 2014. It is called "Cyber Street" and will provide materials and information on how to protect against internet fraud. The initiative looks to highlight the links between careless behaviour and security breaches, direct people to specific prevention guidance on a range of topics and advise individuals and companies on best practice and warning signs to look out for. The Fraud Advisory panel has also developed a factsheet for organisations looking to manage e commerce risk which details good and bad practice. Looking forward the Department for Business, Innovation & Skills is considering the issue of cyber security organisational standards and this may provide for additional sources of guidance.

Wilson: We must begin with the premise that fraud cannot be prevented in its entirety. Where individuals or business owners have a motive and the propensity to commit fraud they will find opportunity. Minimising the opportunity to commit fraud as well as maximising the prospect of discovering fraud or corruption if attempted must be the objective of any fraud prevention system. This system would of course be even better where there is ethical management or regulatory control that takes seriously its steps and action to fight against fraud. This includes the investigation and prosecution where appropriate of all suspected incidents of fraud or corruption reported.

The best an entity can hope for is to improve its probability of discovering

fraud in the normal course of business or through anonymous tips from employees, vendors, suppliers or the public. This requires physical, software and cyber safeguards, division of duties of employees with access (or constructive access) to assets, surprise audits as well as routine comparisons of actual to recorded transactions and other internal control measures designed to detect fraud. We also see that assertive and ethical leadership within entities and governments further improves the likelihood that fraud will be discovered and dealt with assertively thus improving the overall effectiveness of the fraud prevention program.

Hin: Protecting yourself and your data against fraudsters is always important. Estimate the value of your information, your risk appetite and possible risks and determine the necessary controls. And do this continuously. High quality data means often that more controls need to be in place. And nowadays these controls need to be more sophisticated. Some examples of basic controls are:

- perform a regular risks assessment on high quality data;
- have a data security process embedded;
- never store unencrypted passwords;
- 2-tier login where possible (e.g. password and sms);
- always respond on (possible) information theft (close the gap and inform the people involved).

Always keep in mind: security is a continuously evolving process.

Conry: A key issue is how companies that handle data can protect themselves from an attack in the first instance. Data security is very context-specific, so a company should first conduct a risk assessment to identify the issues that are relevant to the type of business that it conducts, its size, the way that it receives data, the type of data it handles, where data is stored—including older data, and any logistical difficulties the company faces. Then, entities should establish a written information security policy that takes into account the current prevailing industry practices and the particulars of that company. Best practices recognise that there is no silver bullet to ensure information security; relying on one type of security measure generally will not suffice. Rather, companies need "defence-in-depth." This means that several layers of protection (such as firewalls, different access controls, intrusion prevention systems, encryption measures, data loss prevention, etc.) should be combined. Because technology and security threats evolve rapidly, companies should also have in place a risk assessment policy that requires periodic analysis of risks and industry standards. Lastly, companies should have an incident response plan so that, in the unfortunate event of an intrusion, they can respond swiftly.

9. Can you outline the advantages that companies receive from using whistleblowing services?

Ratley: ACFE research shows that more fraud cases are detected by a tip than by any other control method. Also, where a fraud hotline was in place, the average duration of a fraud scheme was reduced by seven months and the median loss was reduced by nearly 60 per cent. The obvious lesson here is that companies need to take advantage of this opportunity to detect more fraud. They should provide a process through which employees, contractors and customers can anonymously report suspicious activity. A fraud hotline, for example, makes it easy for whistle blowers to make such reports, and just the very presence of a hotline helps communicate to all employees that the company is serious about detecting fraud.

Corker: Hopefully early warning of improper conduct by middle or low ranking employees. This enables the company to remedy the problem before it escalates. However whistleblowing services is a mixed blessing. The drawbacks are encouraging malicious or ill-informed gossip, obliging the company to investigate every allegation and creating a paper trail that regulators may later demand to see in another context.

Rooyen: The Association of Certified Fraud Examiners 2012 Report to the Nations, highlights that 43 per cent of all occupational fraud is detected by way of tip offs. Management review, the second most prolific means of detection only account for around 14 Per cent. This is a clear indication of the value of employee reporting.

Furthermore whistleblowing also assists companies in developing and encouraging a culture of trust and confidence with its stakeholders. The stakeholders would typically include employers, trade union representatives, shareholders and suppliers, as well as their employees. This culture of trust and confidence will encourage the various stakeholders to report suspicious behaviour at an early stage. By doing so, the company could also improve its brand value as it will be seen by all its stakeholders as an organisation that encourages everyone

to report wrongdoing.

Schwarz: There is a clear advantage of being the first to receive information that is provided by whistleblowers. From a company's perspective, you want to have as much time available to investigate and appropriately respond to whistleblower allegations before they hit the news wire or are reported to the authorities. With new legislation, such as the Dodd-Frank Act, providing incentives to whistleblowers to report to an office outside of the company, it has become a more challenging task for companies to attract good-faith whistleblowers to disclose themselves to the appropriate corporate functions and hotlines. Gaining critical time to get your hands around the facts and prepare your response is the main advantages companies gain from these services. This is a lot in today's short fused world.

Tumani: The first and major benefit is that a company will have the potential to understand, interrupt and properly deal with matters that could severely affect its reputation, regulatory profile and in some cases corporate standing in the eyes of the criminal law. An effective whistleblowing service gives an early insight into problems that might otherwise fester or find an outlet outside of the company. Once an issue is identified a thorough investigation will assist in managing the scope of any subsequent employment, procedural, regulatory or criminal consequences. In serious or difficult cases outside counsel will be able to provide an independent investigation and perspective. In the absence of an effective whistleblowing procedure employees may use the internet or otherwise directly involve regulators. In such circumstances a regulator may take a hostile position towards the company that may be difficult to displace. Finally a whistleblowing procedure provides a means for a company to properly understand and review the effectiveness of its anti-bribery, money laundering or anti-fraud framework.

Wilson: Whistleblowing services provide significant added protection in fraud detection that goes above and beyond internal and external audits. If properly executed and investigated while protecting the anonymity of the tipster, these services provide a critical compliment to the overall control environment of an entity.

According to the ACFE's 2012 Report to the Nations, fraud is discovered through an anonymous tip from customers, suppliers, employees and others was more than three times the incidence of fraud detected by Internal Audit, Management Review or Account Reconciliations and way more effective that the fraud detected by external auditors.

The addition of a program that encourages tips from whistle blowers is an essential component to the protection of the public through its increase in the likelihood that fraud, particularly financial statement fraud, will be detected.

Gurkaynak: Whistleblowing services allow a company to detect its employees' wrongdoings, before the official authorities discover the illegality. A wrongdoing discovered in such manner buys the company time for damage control in order to assuage the possible pernicious effects of a corruption scandal on the company's reputation. Furthermore, the company who has discovered the wrongdoing itself may disclose it to the authorities and possibly benefit from any leniency system if available. On top of that, having a whistleblowing system is actively encouraged both by the FCPA and the UK Bribery Act as a significant part of a compliance program. In the context of the FCPA, a company which did not employ whistleblowing services could fail to get a fine reduction based on its compliance program.

Whistleblowing service also helps a company monitor the application of its own company rules and regulations. If correctly implemented and used, the system runs as a self-detection model enabling a company to control any potential breach of the company rules, laws, regulations, etc.

Rupp: There are differences of opinion, largely for historical or cultural reasons, in different countries concerning the acceptance of whistleblower hotlines – in particular, the acceptance of anonymous reports of non-compliant conduct. If a company is truly committed to operating within the confines of the law, reservations concerning whistleblower hotlines must be overcome. So, too, must the reservations that continue to exist about establishing a no-retaliation policy for reports of potentially non-compliant conduct submitted in good faith. Encouraging whistleblower reports, including anonymous reports, can alert a company to one-off instances of non-compliance before such conduct becomes systemic. They also can and often do alert companies to weaknesses in the company's compliance program,

allowing them to remediate those weaknesses before a little problem has escalated into a very large problem.

Hin: In general, whistleblowing is one of the main means of detecting fraud, bribery or corruption. Therefore, all organisations should have whistleblowing procedures in place. Implementing whistleblowing procedures can be part of the soft control measures to promote the desired culture, leadership and integrity within an organisation. Also, information is becoming more readily available and is easily shared via the internet and social media. Disgruntled employees may express their dissatisfaction via the digital highway. People are able to inform a huge amount of users in a split second. As a result, the number of company complaints, tips and anonymous reports will continue to increase, leading to information being shared at the risk of reputational damage. We advise our clients to pay attention to soft controls in their organisation and mitigate the reputation risks by having preventive instruments such as whistle blowing procedures in place.

10. Governments and regulators appear to be taking tax havens and tax evaders more seriously with an increase in high net-worth individuals and large multinational companies having been investigated. Do you expect to see a continued effort by authorities to tackle this issue or is it simply an uphill battle?

Corker: This is largely an uphill battle because there are too many jurisdictions including the U.S. e.g. Wyoming, Nevada, who operate low regulatory environments in order to attract business. The OECD is doing all it can to promote multilateral and multinational standards but in reality there is a very long way to go before they become effective.

Schwarz: For Germany- in particular, the self-disclosure of tax evasion by Uli Hoeness, the President of the most famous FC Bayern Munich - has triggered another avalanche of self-disclosures and reportedly lead to an increase in tax revenues of approximately €3.5 billion in the last year alone. These are impressive numbers that will drive further enforcement activities. The new German grand coalition government has already committed itself to focus its law making activities in this area and make the respective regime even more rigid. In Germany, tax evasion over the last few years has dramatically moved away from a petty crime that was oftentimes not sanctioned to a mainstream crime that receives high attention. Also the perception in the public as changed and is more focused on seeing offenders behind bars or at least severely fined.

Wilson: The US Justice Department and the current presidential administration have clearly stated that fraud prevention is a priority, which has resulted in an observed increase in cases that are filed and won against perpetrators. As referenced earlier, the administration created a Financial Fraud Enforcement Task Force which has augmented the resources in this area. There is a contemporaneous battle going on in the fight against Cybercrime, which is a significant threat and corollary to the fight against fraud and corruption. It appears that these battlegrounds are testing the available resources of the system to combat them, yet it appears that the US government has the resolve to continue the fight with appropriate resources.

Rupp: The short answer is "yes." The countries or jurisdictions that have built their economies in whole or in part by accepting and protecting from foreign scrutiny undeclared income or ill-gotten gains are decreasing with each passing year, for good reasons. And those reasons are going to shrink the pool of such countries or jurisdictions further over the coming years. If a high net-worth individual is anxious to avoid prosecution, and possible jail time, the best advice I can give would be to declare in a scrupulously accurate manner the income that you actually have received and pay the taxes that are due on that income. There always will be, of course, those having a large appetite for risk but we appear to have reached or very nearly have reached the point at which tax evasion will be limited to people who enjoy jumping from the top of very tall buildings without a parachute.

Rose: Yes. As a result of the recession in the past five years, there has been huger pressure on government revenues. This has led to a review of schemes used by individuals and companies to manage and on occasion evade their tax liabilities. The political attitude towards tax avoidance/evasion is changing and more resources are likely to fund tax investigations. A number of successful prosecutions in the UK and elsewhere have shown that more revenue can be generated by cracking down on evasion and tax minimisation schemes. High profile breaches of bank security in offshore jurisdictions

are likely to continue with increasing levels of international co-operation.

Molo: It is reasonable to assume tax enforcement will remain a priority. Governments are aggressively looking for sources of revenue and there seems to be an attitudinal shift toward viewing tax evasion as both truly serious and worth pursuing in terms of both the taxpayer and those facilitating evasion. One could say the U.S. pursuit of UBS signalled this shift. Additionally, the large rewards available to whistleblowers in U.S. tax laws will promote investigations.

11. To what extend would global accounting standards make international trade cheaper and more accessible to a wider audience?

Molo: Global accounting standards would be a significant plus. At some level, so long as there is a fair set of rules that provide accurate, reliable information to the marketplace, it should not matter greatly whose rules they are. The increasing globalisation of transactions as well as the investing public bode in favour of uniform standards and the IFRS Foundation has been working toward that end for some time. Convergence is a complex process and the SEC and FASB have repeatedly stated and shown a commitment to harmonisation. The momentum is there and the demands of the marketplace will drive this change.

12. What key trends do you expect to see over the coming year and in an ideal world what would you like to see implemented or changed?

Ratley: In addition to cybercrime, large financial frauds and Bitcoin, I also expect to hear more about the crowdfunding phenomenon and how it is sometimes used to fraudulent ends. Crowdfunding is a process in which entrepreneurs appeal directly to potential investors through an online crowdfunding platform, thus avoiding banks, brokers or other intermediaries. Regulators are largely still determining what controls are needed to help weed out fraudulent crowdfunding scams from legitimate investment opportunities.

In an ideal world, there would be no fraud. The reality, however, is that fraud will probably grow before it shrinks. The main thing I wish for is that companies of all sizes and industries take a proactive approach to detection and prevention. Having a comprehensive, well-communicated anti-fraud plan in place is so much more effective than dealing with fraud's aftermath.

Rooyen: Africa has some of the fastest growing economies in the world and Ernst & Young's Africa Attractiveness Survey 2012 estimated that new foreign direct investment projects will amount to US$150bn by 2015, which will ensure a significant amount of acquisitions. As is the case with many new and alluring opportunities, investing in Africa can have its own pitfalls which, if not managed effectively from the outset, can cause an investor untold aggravation. These pitfalls would obviously include fraud and corruption.

The vast majority of the African countries assessed scored below five on a scale of 0 (highly corrupt) to 10 (very clean). As many investors have learnt, the discovery of bribery and corruption after closing an acquisition is one of the fastest ways to lose company value, given that the regulatory and legal fines, penalties and remediation costs can be significant. Of equal significance would be the discovery that the newly acquired company is involved in or the victim of some fraudulent scheme. The bottom line is that if you acquire a company, you acquire its problems as well.

In trying to cope with this situation, many companies have ended up between the proverbial 'rock and the hard place', as the need for local contacts and procedural knowledge to deal with the fraud landscape in Africa leads many companies to engage third-party agents or business partners. Such relationships can expose companies to significant anti-bribery and corruption legislation (ABAC) compliance risks, and often cause more harm than good.

It would greatly assist if a culture is developed where companies focus more on detection and prevention rather than remediation. Standardisation of legislation would further lead to clarity and certainty.

Schwarz: I believe that the flattening of the world, shrinking of distances, and consequently, reduction of response time to compliance issues will continue with an accelerated speed. This creates huge challenges for international organisations to have responses available for upcoming issues in literally "no-time". At the same time, once issues get in the cross-hairs of enforcement agencies, the company finds itself back in the "old world" with protracted, globally fragmented, and – often

times – intransparent, enforcement procedures, that have all the power to blow away company's profits with one compliance enforcement matter. My wish would be to see a narrowing of the gap between the speed in which companies move and operate world-wide these days and the regulators world-wide handling of enforcement activities. However, my expectation is that this gap will keep on widening for some more time.

Tumani: The FCA has now concluded thematic reviews into the Insurance, Investment Banking and Asset Management industries and I expect to see a continued focus by them on money laundering and anti-bribery issues. The SFO has said that it has corporate UK Bribery cases under investigation. It may be that some of these cases will be suitable for resolution by way of DPAs. The SFO will shortly be producing a response to the consultation on how Prosecutors' will make decisions relating to DPAs and the UK Sentencing Council will similarly publish a response to the consultation on corporate punishment for fraud, money laundering and bribery offences. Given these developments it will be interesting to see whether there is a meaningful trend towards a greater use of negotiated outcomes. The Competition & Markets Authority will also be in a position to test the new cartel offence and given that it is now easier to prove there may well be a trend towards greater enforcement activity in the anti-trust field.

Gurkaynak: One of the key trends that occurred in the anti-corruption landscape recently has been the increase in the enforcement of anti-corruption laws in the public sector. Ideally and practically, we expect this trend to spread to the private sector as well. Additionally, within the scope of Turkey's Financial Action Task Force membership, we expect further enactment and rigorous enforcement of the money laundering laws.

Finally, with regard to the enforcement of anti-corruption laws, it would be preferable for Turkey to create a central anti-corruption enforcement agency independent from any governmental authority having its own budget. Turkey would benefit from more frequent and swifter anti-corruption investigations if enforcement agencies such as the Financial Crimes Investigation Board and the Prime Minister's Investigation Board operated in a coordinated manner.

Hin: Within the next years we expect more and more (social) data will be recorded by companies because people are increasingly (unconsciously) willing to provide this data. The concepts of social media and business data will further integrate, so social media will eventually become business data (Big data). Regulations regarding privacy are going to be expanded, but the effectiveness will decrease. The growth of technical possibilities and the loss of privacy awareness will lead to the loss of privacy and control of your own data. In an ideal world you are always in control of your own data. To make this possible, all data is stored decentralised and each person is carrying their own data. When another person wants to have access to your data, you can give temporary review access to it. And after a certain period of time the provided review rights to the data will be disconnected.

Rose: There is a growing level of cooperation between the regulators in Europe, the US and the Asia-Pacific. Information is being shared, strategies are agreed and penalties determined on a cross-border basis. Simultaneously there is a growing disparity in the way in which companies and individuals are treated. Given the different resources available to people and entities and the threat that individuals face of financial ruin and or prison the need to ensure procedural fairness is greater than ever.

Conry: Over the last year and a half, the Department of Justice ("DOJ") has begun requiring that some corporate defendants in health care fraud cases agree to take on compliance commitments as part of their negotiated criminal resolutions. In some cases, these compliance obligations have been styled as terms of probation, while in other cases, the terms are contained in a side letter. This new type of compliance agreement is separate from a Corporate Integrity Agreement ("CIA"), and obligations run to the Probation Department or the DOJ rather than the Department of Health and Human Services. I would like to see this trend cabined, and used only when a particular case calls for it, in light of a company's pre-existing compliance structures and/or CIA. Further, when terms are imposed, they should be tailored to take into account the facts of the case, and not imposed merely because they were part of a prior agreement.

Molo: Look for stepped up antitrust and anti-corruption enforcement. The successful cooperation among countries in these endeavours will breed cross-border investigations in

other areas such as serious frauds and tax evasion.

As far as changes – simplification and harmonisation of privacy rules would lessen the cost and effort in defending, not to mention pursuing, these matters. Additionally, international agreements on the reach of amnesty and self-reporting protections could promote a more certain landscape.