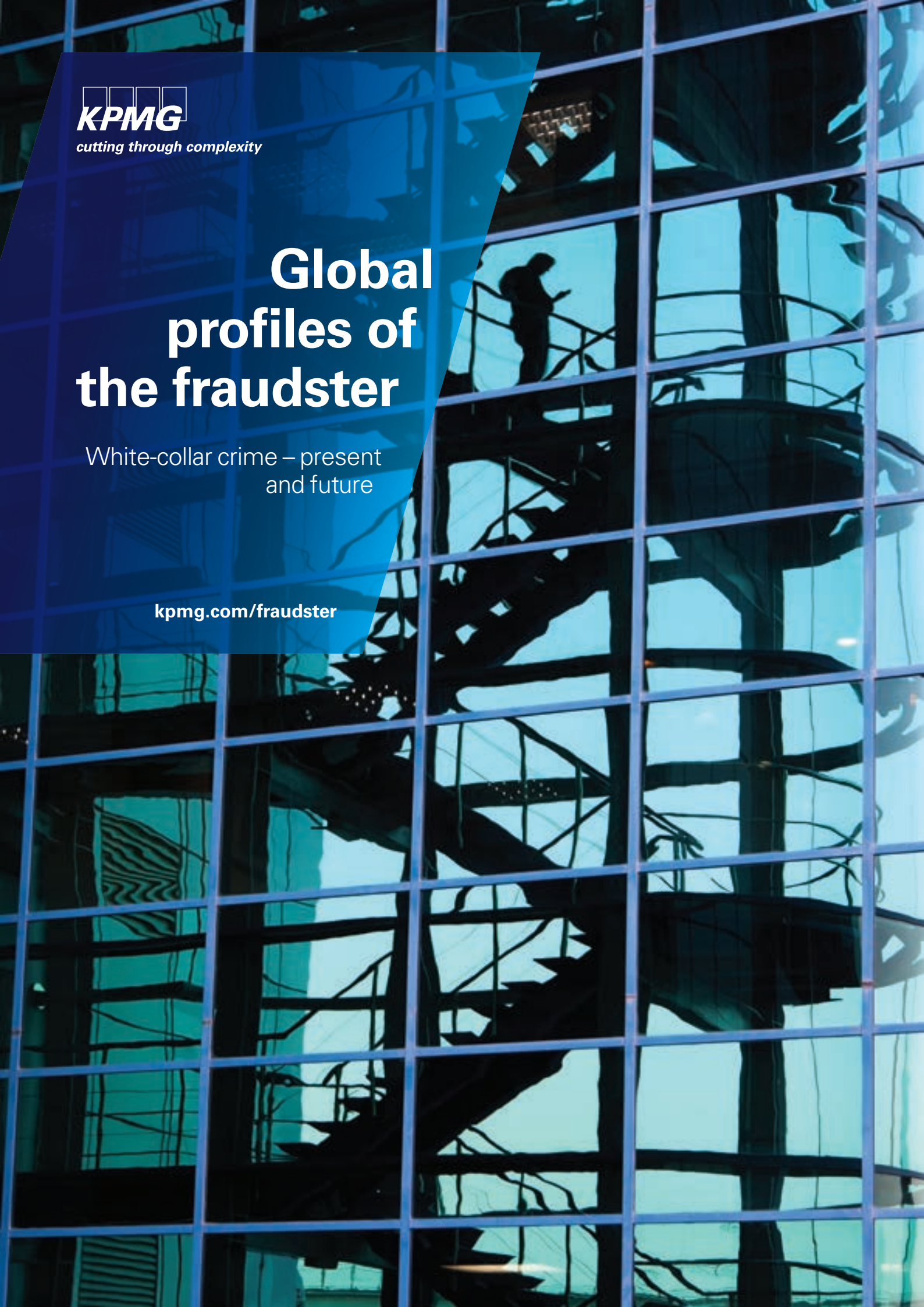


KPMG
cutting through complexity

Global profiles of the fraudster

White-collar crime – present and future

kpmg.com/fraudster

Introduction

Fraud specialists have long debated whether it is possible to develop a profile of a fraudster that is accurate enough to enable organizations to catch people in the act of fraud or even beforehand. The prediction of a crime before it occurs is, at least for now, the subject of science fiction. But an analysis of the constantly changing nature of fraud and the fraudster can help organizations stiffen their defenses against these criminal activities. Forewarned is forearmed.

This report contains KPMG's analysis of 596 fraudsters member firms investigated between 2011 and 2013. It is intended to provide the reader with insights into the relationship between the attributes of fraudsters, their motivations and the environment in which they flourish. We have also interviewed KPMG member firms' investigation leaders to gain additional insights. This report builds on our 2011 publication, *Who is the typical fraudster*?[1] covering 348 cases investigated, and on our 2007 publication, *Profile of a fraudster*.[2] *The 2011 report* focused on the relationship between global patterns of fraud, various attributes of fraudsters and how these may evolve in the next five years.

The typical fraudster among the 596 included in the 2013 survey is very similar to the typical fraudster identified in the investigations KPMG firms reported on two years earlier. The typical fraudster in the 2013 study is 36 to 45 years of age, is generally acting against his/her own organization, and is mostly employed in an executive,[3] finance, operations or sales/marketing function. He/she holds a senior management position, was employed in the organization in excess of six years and, in committing the fraud, frequently acted in concert with others.

Other findings, however, are different. This time, we have developed a series of themes in order to understand the changing relationship among the fraudster, his/her environment and the frauds committed. And after taking into account the insights of our investigation leaders around the world, we conclude that the type of fraud and the type of fraudster are continually changing. "The intriguing thing about fraud is that it is always morphing, like a strain of flu; you can cure today's strain, but next year it evolves into something as bad if not worse," says Phil Ostwalt, Global Coordinator for Investigations for the Global Forensic practice at KPMG.

The typical fraudster among the 596 included in the 2013 survey is very similar to the typical fraudster identified in the KPMG investigations reported on two years earlier.

One major change is the growing use of technology by fraudsters, and not just in the technologically advanced countries, such as the US "a concern for all business is that we are about to see a new generation of people, able to use more technology and with access to much more information than past generations. All of which points to a new era for fraud and illegal activities," says Arturo del Castillo, Managing Director of Forensic, KPMG in Colombia.

We believe that understanding this fluidity will enable organizations to protect themselves better against fraud and may improve their ability to identify the fraudsters, many of whom perpetrate their crimes over long periods. A lot of fraudsters are hiding in plain sight. They may blend into the background or occupy prominent

[1] Who is the typical fraudster? KPMG analysis of global patterns of fraud, 2011
[2] Profile of a fraudster survey, 2007
[3] The function is also known as general management and includes the Chief Executive Officer.

positions in the organization. The types of fraud they perpetrate are continually changing, amid a business environment in constant flux.

New fraud techniques are continually developed and organizations need to respond by updating their defenses. "Companies can't stand still and allow yesterday's controls to address today's or tomorrow's fraudster," says Ostwalt. Technology not only enables the fraudster, but also enables the organization to defend itself. "Companies have to think harder about whether old fraud prevention technologies still apply. Newer approaches like data analytics and data mining give the company a much better chance of catching the fraudster," says Grant Jamieson, partner in charge of Forensic Services for KPMG in Hong Kong.

Read on to find out more about the frauds member firms investigated globally since the 2011 report, our analysis of the changing profile of a fraudster, how it relates to their environment and the crimes committed, and our views of what fraudsters may look like and how they might behave in the future.

Based on KPMG's analysis of the 596 fraudsters member firms investigated, some of the key characteristics of fraudsters include:

- Age – 70 percent of fraudsters are between the ages of 36 and 55
- Employment – 61 percent of fraudsters are employed by the victim organization. Of these, 41 percent were employed there for more than 6 years
- Collusion – In 70 percent of frauds, the perpetrator colluded with others
- Type – The most prevalent fraud is misappropriation of assets (56 percent), of which embezzlement comprises 40 percent and procurement fraud makes up 27 percent
- The second most prevalent fraud is revenue or assets gained by fraudulent or illegal acts (24 percent)
- When fraudsters acted alone, 69 percent of frauds were perpetrated over one to five years. Of these, 21 percent of the frauds incurred a total cost to the victim organization of $50,000-$200,000 and 16 percent cost a total of $200,000-500,000. In 32 percent of these cases the cost to the victim organization exceeded $500,000, exceeding $5,000,000 in 9 percent of these cases
- When acting in collaboration, 74 percent of frauds were perpetrated over one to five years. With regard to value, 18 percent of frauds had a total value of $50,000-$200,000. In 43 percent of these cases the cost to the victim organization exceeded $500,000, exceeding $5,000,000 in 16 percent of these cases
- 93 percent of frauds were committed in multiple transactions. For 42 percent of these frauds, the average value per individual transaction was between $1,000 and $50,000
- 72 percent of all frauds were perpetrated over a one-to-five year period (33 percent over one to two years and 39 percent over three to five years).

Methodology

By means of a survey, KPMG gathered data from fraud investigations conducted by KPMG member firms' forensic specialists in Europe, Middle East and Africa (EMA), the Americas, and Asia-Pacific regions between August 2011 and February 2013. We analyzed a total of 596 fraudsters who were involved in acts committed in 78 countries. The survey examined "white collar" crime investigations conducted across the three regions, from interviews from 42 KPMG Forensic practitioners, where we were able to identify the perpetrator and could provide detailed contextual information on the crime.

The analysis identifies:

- Fraudster profiles and details of the more common types of fraud
- Environment considers that tend to enable fraud
- The impact of fraudster's capabilities
- The context in which fraudster's ply their trade across the countries in which KPMG operates

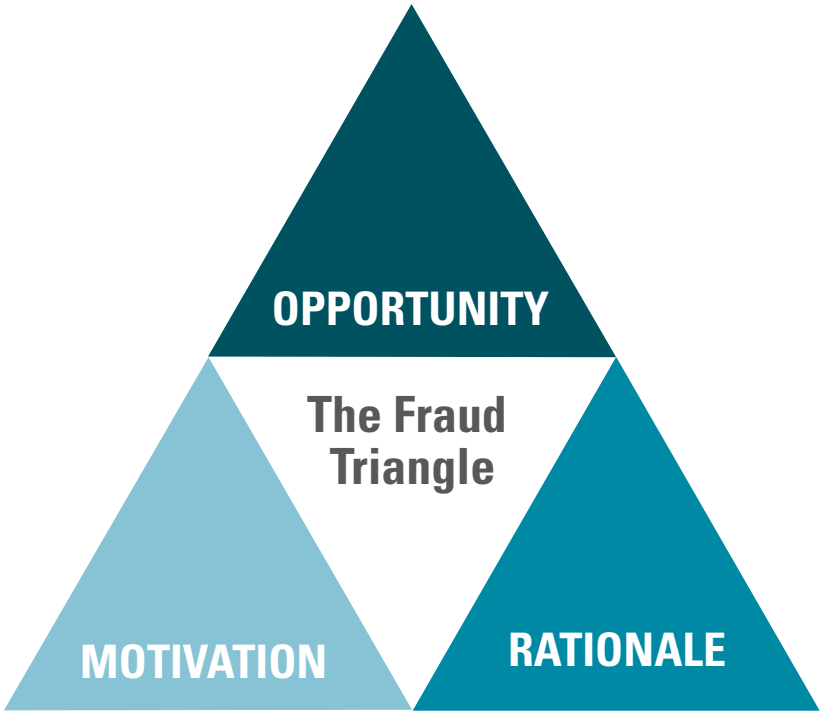
The findings in this report are contrasted, where possible, with our 2007 and 2011 analysis to highlight shifts in patterns and to provide a perspective on emerging trends.

This report does not reveal the names of any parties involved to protect confidentiality. Many of the cases included here did not enter the public domain; others were publicized but usually without the details. All monetary amounts are reflected in US Dollars.

Three drivers of fraud

In order to understand a fraudster's profile it is useful to consider three drivers of fraud: opportunity, motivation and rationale. "People commit fraud when three elements occur simultaneously, the perfect storm; motivation, opportunity and ability to rationalize the act. In almost all cases, this explains why the fraud occurs and why a particular type of person becomes a fraudster," says KPMG's Forensic practice in China. The three drivers are part of a standard methodology developed for fraud investigators in the 1950s. We include capability as a component of opportunity to create a more complete picture of the person who commits fraud. Here is one way to understand the picture: The potential fraudster sees a door opened by opportunity. Motive and rationale propel him/her towards the doorway and capability takes him/her through it.[4]

The Fraud Triangle



Source: Global profiles of a fraudster, KPMG International, 2013.

[4] See *Beyond the fraud triangle*, Fraud Magazine, September/October 2011.

> Having good internal controls is important, but with any control you are ultimately relying on the human element.

Niamh Lambe
Director of KPMG, Head of KPMG Forensic Ireland

Now, let us look at each of the drivers of fraud in turn:

Opportunity

People do not commit fraud without an opportunity presenting itself. A plurality of fraudsters in the surveyed cases investigated have worked in the victim organization for more than six years, and nearly three quarters of the frauds were conducted over a 1-5 year period. This implies that fraudsters do not join an organization with the aim of committing fraud. But changes in personal circumstances or pressures to meet aggressive business targets may create the conditions conducive to fraud. They may commit the fraud once they are comfortable in their job and enjoy the trust and respect of colleagues (see sidebar).

> Management frequently regards fraud risk as a single dot on the risk matrix, not always fully appreciating its real nature and extent.

How does the opportunity present itself? According to the survey, 54 percent of the frauds were facilitated by weak internal controls. This suggests that if many organizations tightened controls and the supervision of employees, the opportunity for fraud would be severely curtailed. Too often, organizations do not focus on fraud prevention by setting up the right controls and learn their lesson too late.

"Many companies think of proactive anti-fraud measures like insurance – if it may never happen, why spend the money?" says James McAuley, Partner, Forensic, KPMG in Canada. Elsewhere, organizations lack even simple controls. "Frauds frequently occur because of a failure to have a basic control in place. Our investigations show, for example, that management does not always check supporting documentation before authorizing a transaction. This goes back to Sweden's culture of trust," says Martin Krüger, Partner in charge of Forensic for KPMG in Sweden. In parts of the Middle East, many organizations are only beginning to understand the need for controls to prevent fraud. "We see many public and privately owned companies exposed to fraud, with few defenses. Although internal controls and fraud risk management is not yet embedded in the business culture, the

Opportunistic fraudster

- Characteristics: first-time offender, middle aged, male, married with children, trusted employee, in a position of responsibility, good citizen in community
- Typically has a non-sharable problem that can be solved with money, creating perceived pressure
- When discovered, others are often surprised by the alleged behavior of the perpetrator

Predator

- Often starts as an opportunistic fraudster
- Alternatively, seeks out organizations where he or she can start a scheme almost immediately upon being hired
- Deliberately defrauds organizations with little remorse
- Better organized than the opportunistic fraudster and with better concealment schemes
- Better prepared to deal with auditors and other oversight mechanisms

dialogue has started," says Arindam Ghosh, Associate Director and Head of Forensic Services, Risk Consulting, KPMG, in Bahrain and Qatar.

But strong internal controls will not prevent all fraud. For 20 percent of the fraudsters, the fraud was committed recklessly, regardless of the controls. And for 11 percent, fraudsters colluded to circumvent the controls. In these cases, the fraudster may be somebody who understands the controls and knows how to manipulate them or who finds a flaw in the controls by accident and exploits them. No control system is watertight. Human vigilance is required. KPMG's investigators say that organizations need to monitor continuously the internal and external environment, yet they have found that most of them do not do this. "Management frequently regards fraud risk as a single dot on the risk matrix, not always fully appreciating its real nature and extent. This often means it is not then given the attention and treatment required to manage the risk," says Mark Leishman, Partner, Forensic Services, KPMG in Australia.

Sanctions, such as civil litigation or public prosecution, may deter fraud, but few companies are prepared to risk harm to their reputation. A jail sentence was the fate of only 7 percent of the fraudsters, while criminal or civil litigation proceedings was for 35 percent. Fifty-five percent of fraudsters were dismissed from their jobs, thus raising the risk that fraudsters may commit crimes at other companies where they are subsequently employed in the absence of being prosecutured. All the more important, therefore, to establish regulations to control business behavior and then to enforce them. "In Singapore, relatively speaking, there is very little corruption, mainly because the enforcement is stringent, and business is conducted in a transparent way," says Lem Chin Kok, Partner, KPMG Forensic Services, KPMG in Singapore.

In Singapore, relatively speaking, there is very little corruption, mainly because the enforcement is stringent, and business is conducted in a transparent way,

Capability

As noted earlier, we include capability as a subset of the opportunity driver. Capability consists of those attributes of the fraudster that enable him/her to exploit the opportunity, when it arises. The attributes are the fraudster's personal traits and his/her ability to execute the crime.

Capability often depends, therefore, upon the seniority of the fraudster. A large proportion of fraudsters holds managerial or executive positions[5] (25 percent and 29 percent respectively of those employed by the victim organization). "In the next 3 to 5 years, we may see the fraudster in the East Africa region becoming increasingly sophisticated and senior in the organization as company controls improve, and more fraudsters are successfully tried and sentenced," says Marion Barriskell, Head of Investigations for KPMG in East Africa. The more senior the fraudster, the greater the ability to get past controls. "We usually find the fraudster overriding controls. While most companies in Switzerland have standard internal controls, a person can root out opportunities after 4 or 5 years," says Anne van Heerden, Partner in charge of Forensic and Consulting practices for KPMG in Switzerland.

Among those insiders who collude with other employees, the respective ratios are 24 percent and 38 percent.

[5] As noted earlier, KPMG tends to investigate frauds perpetrated by senior employees, so this finding may not hold among the entire population of fraudsters, in which there may be a high proportion of crimes committed by lower-level employees.

Fraud by industry

In every industry, fraud tends to be shaped by the opportunities for malfeasance. In financial services, pharmaceuticals, consumer and industrial markets, the most common fraud is embezzlement. But in energy & natural resources (ENR), the public sector and information, communications & entertainment, the most common fraud is procurement. Financial services yielded the highest cost of fraud, commonly more than $5 million per fraudster. Other industries suffered lower costs, often in the $200,000 - $500,000 range. Corruption was more prevalent in pharmaceuticals, financial services and ENR than in other industries. In the case of pharmaceuticals and financial services, this occurred despite the fact that organizations in these industries operate in a highly regulated environment.

Second, 46 percent of all fraudsters were computer literate, which is increasingly an asset when so much data is stored in computers and when cyber fraud is likely to grow in frequency. In terms of personal traits, the preponderant characteristics do not tend to support the notion of a reclusive loner. The fraudster tends to be highly respected (39 percent of all cases surveyed), friendly (35 percent) and/or extroverted (33 percent).

Motivation

Fraud, as with any crime, requires a motive, and for the 596 fraudsters, the overwhelming reason for committing fraud is financial. The survey respondents were offered 14 possible motivations and could select as many as they believed appropriate. Out of a total of 1,082 motivations listed, 614 were motives of greed, financial gain and financial difficulty, and a further 114 were related to business targets. The only non-financial motive that comes close is sheer eagerness (or "because I can") with 106.

These 614 motivations cover a wide range of financial triggers. One such is a desire to enhance one's lifestyle. "Typically, a person commits fraud to fund an extravagant, or at least very comfortable, lifestyle; we seldom see people turn fraudster to make ends meet. Already well off, we often wonder why they take the risk," says Anne van Heerden, Partner and Head of Forensic for KPMG in Switzerland. Other financial triggers include the fear of missing a financial target or the desire for a bigger bonus. "More foreign companies are increasing local management's incentives linked to performance and cutting formal earnings. We see this triggering increased earnings manipulation and financial statement fraud, as managers chase targets," says Jimmy Helm, Partner and Head of Forensic for KPMG in Central and Eastern Europe.

Indeed, several investigations leaders noted an increase in earnings manipulation, no doubt related to the effects of the economic recession. "With the economic pressures, several companies facing bankruptcy and, unable to meet stringent targets set by financial institutions, have been resorting to financial-statement fraud or earnings manipulation to demonstrate growth," says Yvonne Vlasman, Partner, Forensic, KPMG in the Netherlands.

Greed infrequently seems to spill over into observable patterns of behaviour. Only 18 percent of the fraudsters had expensive hobbies and 17 percent drove expensive vehicles, hardly distinguishing features when the fraudster is a senior executive.

Rationale

Fraudsters, as with other types of criminals, will frequently provide a rationale for their deeds. Emotional motivators such as anger and fear were mentioned infrequently among fraudsters. Anger and fear were important factors in 10 percent or less of the 596 fraudsters. Even a sense of being under-remunerated was mentioned as important in only 16 percent of the investigations, somewhat surprising since financial gain is an overriding factor in fraud.

The only emotion that appears to be significant is a sense of superiority, which is important for 36 percent of the fraudsters. This may be linked to the fact that 29 percent of the frauds were committed by executive directors, the largest single job title. Indeed, 44 percent of executive directors felt a strong sense of superiority, no doubt reinforcing their view that they did not need to play by the rules regulating the behavior of the rest of the workforce.

As observed by KPMG firms' investigators, the reason for the fraud is broadly determined by the ethical and cultural context, and this varies from country to country. Government regulation and the enforcement of the rules can often reinforce ethical standards, because a fraudster who is prosecuted will find it harder to rationalize his/her actions by saying that the behavior is accepted in the country. "A decade ago in parts of Europe, companies could deduct bribes in foreign jurisdictions as a useful cost. However, what was previously permitted and considered a cost of doing business is now illegal; people will need to change their habits, led, rather than trailed, by legislation," says Gert Weidinger, Partner in charge of Forensic Services for KPMG in Austria.

In some East African countries, business rules are being tightened and more money spent on prosecution of fraud, and malfeasance is becoming less and less acceptable. "Over recent times, there is a decreasing tolerance for fraud as new governments promote freedom of speech and invest in the country's enforcement framework. The attitude towards fraud is changing, from grass roots to business and government; fraud is less acceptable. In short, the window on endemic corruption is slowly closing," says Barriskell. In Vietnam, there are signs of stronger enforcement, too. "Kickbacks and bribes in procurement are widespread; it is part of how business works in Vietnam, and often considered harmless compared to fraud or theft. But we expect tangible outcomes in the next 3-5 years from the increased emphasis on reducing fraud," says John Ditty, Chairman of KPMG in Vietnam and Cambodia.

Nature versus nurture

The relative impact of personal and environmental factors on the propensity to commit fraud

It is important to understand whether personal or environmental factors are stronger determinants of fraudulent conduct, because this finding will influence the way fraud is investigated and how the risk of fraud is managed. If personal factors are dominant, fraud investigations (and fraud risk management) will focus on the fraudster's personality. If environmental factors are dominant, the investigation will focus on the environmental aspects to determine how a fraud occurred.

We isolated those fraud cases KPMG member firms investigated in which we were confident that corrupt conduct was present. Corrupt conduct in the execution of fraud provides markers that helped build a profile of how fraudsters behave in a way that introduces corruption into their crimes. These markers consist of certain behavioral patterns of a specific type of fraudster and help enable the prediction of corrupt behavior as a profile element of a fraudster. In analyzing the corrupt conduct, key observations were grouped into the three drivers, adding for consideration capability as a subset of opportunity (opportunity, motivation, rationale and capability; the first two categories are environmental factors, the latter two are personal attributes).

For 53 percent of the 198 fraudsters where corrupt conduct was present, weak internal controls contributed to the perpetration of the fraud. Internal control is, however, not a strong factor influencing whether a person would engage in corrupt behaviour. Corrupt behaviour involves at least two people, and at least one of them is rarely subject to internal controls. The increasing globalization of organizations is making it more and more difficult for the central office to monitor what far-flung departments are doing. "In the UK more than 60 percent of bribery and corruption investigations relate to problems in other jurisdictions. This is not about more or less corruption in different countries, but the fact that the further away from head office you go, the more the message dissipates, especially in the face of significant pressure on people to achieve results," says Alex Plavsic, Head of Forensic for KPMG in the UK.

More relevant, perhaps, is the nature of the authority under which the fraudster operated. For 62 percent of the 130 fraudsters analyzed where we could observe the degree of authority enjoyed by the fraudster and where corrupt behavior was involved, we found the fraudster had unlimited authority over the domain in which the fraud occurred (whether the domain be the right to sign contracts, authorize payments, and so on). "We continue to see the archetypal fraudster in most fraud investigations in Central and Eastern Europe to be a senior executive or manager with authority, and having been with the company for over 4 years, knowing the system and its weaknesses. What has changed is more collusion, more recklessness," says Helm.

In this sense, unlimited authority reflects a lack of internal controls, albeit in the governance of the domain in which the fraud occurred. We observe that in 61 percent of the 214 fraudsters with unlimited authority KPMG member firms investigated, the frauds occurred in a weaker regulated environment. Thus, the environmental themes of controls and checks and balances are central to three of the four categories mentioned above (opportunity, motivation, rationale; the other one being capability). "Fraud is most common in smaller, family-owned enterprises mainly because they lack the controls to protect themselves against potential fraud. Yet these kinds of companies form the core of the Greek economy," says Christian Thomas, Partner, Head of Forensic for KPMG in Greece.

> Ultimately, it is a tough challenge to investigate cases and to deter bribery and corruption in foreign countries. For many companies it is difficult to get to the other side of the world and to fully appreciate the risks in local environments.

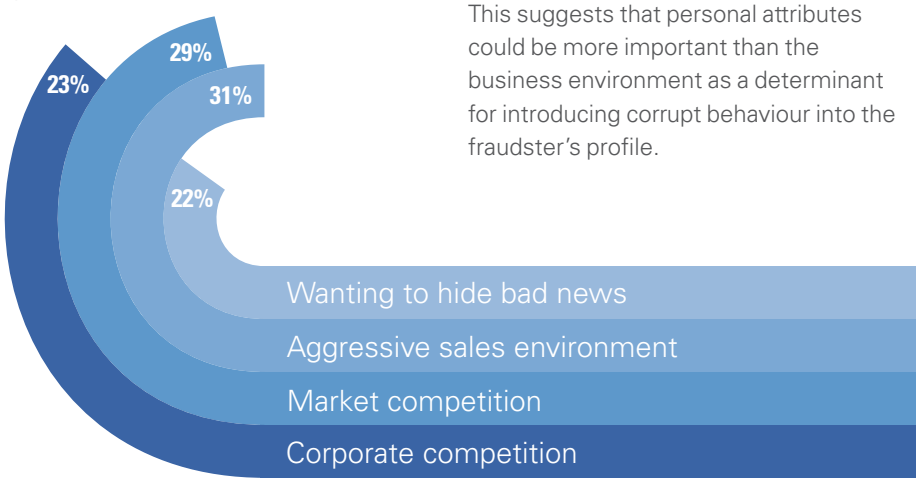
Phil Ostwalt
Global Coordinator for Investigations for the Global Forensic practice at KPMG.

We consider four factors – corporate competition (that is, rivalry among colleagues), market competition (that is, one company competing with another), an aggressive sales culture, and the desire by the fraudster to hide bad news – that are partly environmental, but we judge them to be more closely associated with personal attributes of corrupt behaviour. A fraudster is making a choice about whether and how to respond to these environments, for example, by trying to outdo his/her rivals to earn the highest sales commission. In certain cases, a feeling that "everybody does it" can breed fraud. "A KPMG survey[6] showed that almost all companies believed their competitors would violate ethical standards to obtain business," says Raul Saccani, Senior Manager, Forensic, KPMG in Argentina.

However, based on the data, we were not able to say with confidence that any of these four factors were motivators or pressure points for the 198 fraudsters who behaved corruptly. The occurrences of these factors are set out in Figure 1.

The results of our survey therefore indicate that factors relevant to pressure and motivation have a weaker influence on a fraudster's propensity to behave corruptly than factors relevant to opportunity. For example, if a fraudster needs to establish a collusive network to defraud a company, he/she may have to bribe company officials to do so. In other words, when the fraudsters had the opportunity to behave corruptly when committing the fraud, they did so; it was not a matter of necessity or motivation. This suggests that personal attributes could be more important than the business environment as a determinant for introducing corrupt behaviour into the fraudster's profile.

Figure 1



Source: Global profiles of a fraudster, KPMG International, 2013.

[6] KPMG Report Corporate Fraud in Latin America 2008-10, published in 2011.

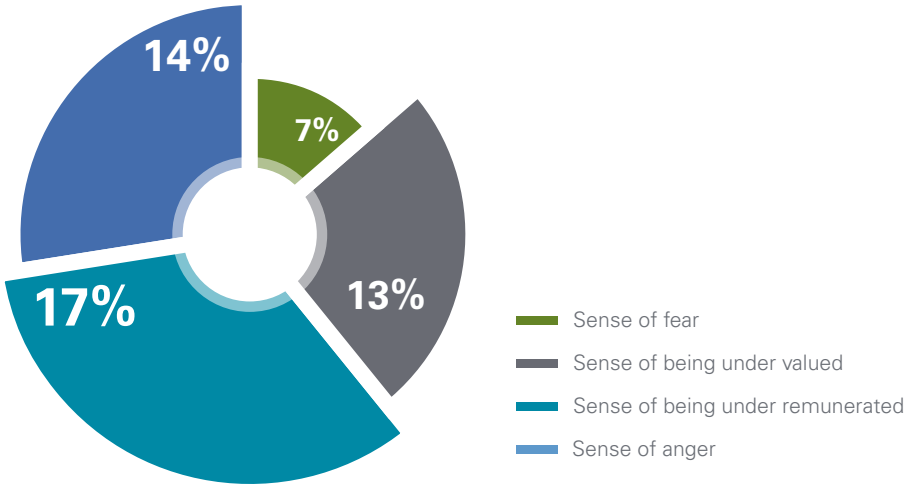
Personality and capability

Next, we consider aspects of a fraudster's personality and capability. We first considered factors relevant to creating a rationale for frauds involving corrupt behaviour and found that emotional motivators (such as anger, fear and resentment) were rarely mentioned as a rationale for the fraudsters' conduct. Some of the emotional motivations are reflected in Figure 2.

Turning to the personal traits and ability of the fraudsters in the cases we investigated, we firstly grouped together observations of their personality and presence.

Given the high proportion of fraudsters that are extroverted, friendly, highly respected, and so on, it is hard to imagine that these attributes could help identify a fraudster with a propensity toward corruption. Furthermore, a large proportion (39 percent) of all 596 fraudsters was highly respected by their peers." The fraudster we encounter is usually the trusted manager or employee in finance; when revealed, most people are surprised, finding the behavior totally out of character," says van Heerden. In Figure 3 we reflect some of the attributes indicating a trusted person like the one referred to by van Heerden.

Figure 2



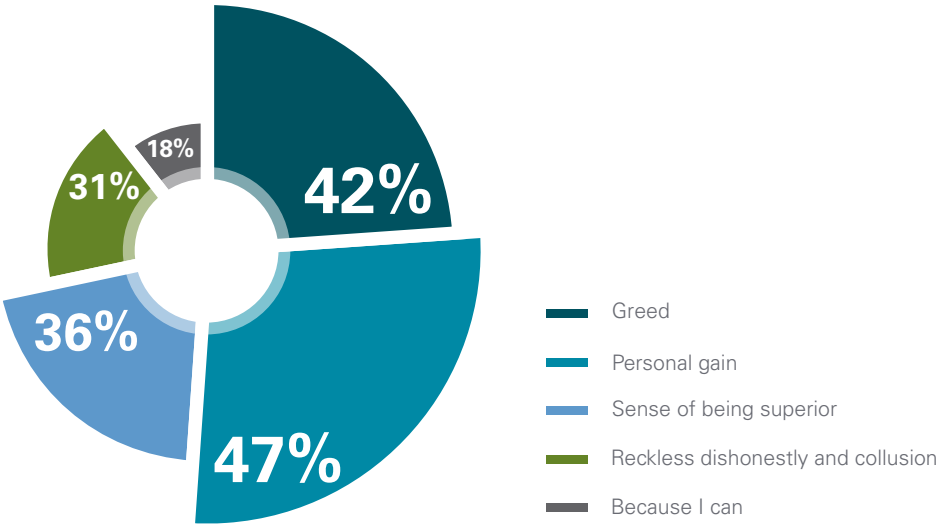
Source: Global profiles of a fraudster, KPMG International, 2013.

Figure 3

Source: Global profiles of a fraudster, KPMG International, 2013.

Greed, reflective of a higher level of moral turpitude, and personal gain were the most prevalent personal traits driving the fraudster's conduct in cases where there was corrupt behaviour. When considering all the 596 fraudsters investigated by KPMG member firms, personal gain on the part of the fraudster was observed in 47 percent of the fraudsters and greed in 42 percent. Therefore, when there is a weakening of internal controls and of governance, ordinary people may become susceptible to greed and to ideas of personal gain. Such people may become marginally more prepared to introduce corrupt behaviour into the fraud they commit than they would otherwise. "What it always comes back to is that fraud is about people, what they want and how much resistance they face. This usually comes down to pursuit of a lifestyle, what is culturally acceptable and the quality of a company's defenses," says Sukdev Singh, Executive Director of Forensic for KPMG in Malaysia.

Figure 4



Source: Global profiles of a fraudster, KPMG International, 2013.

The changing face of fraud

Organizations must adapt to the fraudster's ever-changing profile

There is no single template for fraud and there is no single, unchanging face of the fraudster. The crime and the perpetrator will vary depending on the relative importance of the three fraud drivers and capability of the fraudster noted earlier, and this is often the reason why it is difficult to detect fraud. "We do not see one personality profile that commits fraud; all types of people commit fraud if the opportunity presents itself," says Nigel Layton, Partner, Head of Forensic, Risk Consulting at KPMG in Russia and the CIS. Lem puts it another way: "Our experience shows that most people can commit fraud if confronted with the right trigger."

Given the rather chilling finding that most people are capable of committing fraud, it behooves the organization to make it as difficult as possible for the fraud to occur. "There are no indications as yet that the profile of the fraudster is about to change radically in the near future; it could be anyone, depending on who has the opportunity on the day. The key to unlocking a company's fraud risk is finding ways to change behavior," says Ghosh. One important change in the profile is the expanding role of collusion, as we see in the next section.

Collaborators, insiders and outsiders

Solos are a tough act. Many fraudsters may prefer to work alone, because they do not have to rely on others to keep quiet and to share the spoils with, but most fraud requires collaboration. The fraud is often too complex for one person to execute; it requires others to turn a blind eye, or to provide passwords or falsify documents. A full 70 percent of the 596 fraudsters KPMG professionals analyzed for this report acted in concert with others and, of these, 56 percent involved 2 to 5 other people. Three quarters of fraudsters investigated acted as the principal.

> A full 70 percent of fraudsters in our survey acted in concert with others and, of these, 56 percent involved 2 to 5 other people. Three quarters of fraudsters investigated acted as the principal.

Collusion takes many forms; it occurs both inside and outside organizations. Third-party fraud can be particularly hard to uncover. "We frequently see agents or third parties like customs agents pay a bribe on behalf of a company, then invoicing for apparently legitimate services to refund this outlay. The invoice to the company looks like a legitimate fee for services so it is difficult to detect," says Layton.

When a fraudster colluded, 21 percent of the frauds were embezzlement, compared with 27 percent when the fraudster acted alone. Procurement fraud was the second most common type involving collusion, with 19 percent. Fraud involving collusion does more financial damage, too. Thirty-three percent of cases involving collaboration entailed a total cost to the victim organization of more than US$1 million. For solos, 24 percent involved more than US$1 million.

Collusion appears to be a growing trend. The proportion of cases involving collusion rose from 32 percent in the 2007 survey, to 61 percent in 2011 and 70 percent in 2013. Regionally, however, the picture is less clear-cut. Between 2011 and 2013, there was an increase in the proportion of cases involving collusion in the EMA and Asia-Pacific regions, but not in the Americas. Collusion tends to be higher in countries where business is often driven by social relationships, such as Africa and parts of Asia. But in more patriarchal places, fraud is often committed by senior personnel instructing their underlings to carry out illegal transactions. "People sometimes help perpetrate a fraud not for any personal benefit but because they are told to," says Jamieson.

Insiders and outsiders

An important form of collusion is between the insider and the outsider, especially when it is procurement fraud, such as inflating invoices. Indeed, many organizations fail to conduct due diligence of their suppliers and corporate customers.[7] "The ultimate defense in today's environment is to ask whether you are doing business with and through people you can trust," says Plavsic. For 43 percent of fraudsters, the collusion involved both insiders and outsiders, and for a further 19 percent, the collaboration consisted of a sole insider and one or more outsiders. KPMG firms' investigators say that in most of these cases where insiders worked with outsiders, it was the insiders who took the lead, since he/she tends to identify the opportunity and to know the soft spots in a company's defenses. Indeed, more than 42 percent of fraudsters had worked for the victim organization for more than six years.

Corruption was a common element in cases of collusion; we found 29 percent of collusion-related cases involved bribery (which cannot be present when people act alone). There was also a disparity in the method of detection. Solos were predominantly detected by management review (27 percent) and by accident in a quarter of the cases. When there was collusion, the top fraud detection methods were by anonymous informal tip offs (22 percent) and by formal whistle blowing (19 percent).

> Fraud involving collusion does more financial damage, too. Thirty-three percent of cases involving collaboration entailed a total cost to the victim organization of more than $1 million. For solos, 24 percent involved more than $1 million.

If cyber fraud becomes more important, as seems likely, it remains to be seen whether the prevalence of outsiders will grow. In theory, more hackers will be looking for the weak points in organizations' defenses, but they could be insiders just as much as outsiders. We now turn to the growing role of technology in fraud.

[7] *Third-party risk management: What you don't know about your business partners can hurt you*, KPMG 2013

Adventures in cyber space

New technology has created novel types of fraud behavior

Cyber security has become a buzzword at an alarmingly rapid rate. Much of the publicity surrounding the term has focused on reports of government attempts[8] to impede the development by other governments of nuclear weapons and similar strategic events. But companies find themselves increasingly vulnerable to cyber attacks, many of which, we must assume, go unreported. "The worrying thing about cyber-attacks and high-tech fraud is that it is so easy for perpetrators to gain access; many companies don't even know it is happening," says Vlasman.

Organizations, corporate or otherwise, are struggling to keep pace with the growing technological sophistication of hackers. "While some sectors are better prepared for cybercrime than others, companies that have experienced high-profile cyber incidents do not necessarily appear in a better position to deal with future attacks. These companies are also struggling with how to manage this risk proactively," says Ostwalt.

A few years ago, hackers were motivated by political objectives and disrupted computer networks to make an ideological point; but it's only a matter of time until fraudsters harness the full power of technology to enrich themselves and criminal organizations, unless legitimate organizations take steps to defend themselves. "Computer and network technologies make it possible for white-collar criminals to operate more efficiently and with less risk; it eases access, effectively lowering barriers for a new generation of fraudsters," says İdil Gürdil, Head of Risk Consulting for KPMG in Turkey.

Growth in store

At this point, the scale of detected cyber fraud[9] appears to be small. Of the cyber-related crimes we analyzed, most occurred by way of methods used such as infections of computer systems with malware, attacks on computer networks and so on. Weak internal controls often facilitated the fraud which comprised, inter alia, fraudulent financial reporting and misappropriation of assets. The fraudsters were mostly employed by the victim organization, mainly in IT, but also in finance and operations. They ranged in seniority from staff level to executives, were aged between 18 and 55 years, and were employed by the organization for between one and six years. In most cases they also acted in collusion with others, who were also mostly employed by the victim organization.

Interviews with member firms' investigators suggest that cyber fraud is likely to become a rapidly growing problem for organizations and will take place on a much greater geographical scale than before. "Cyber crime has increased and we expect cyber-attacks and high-tech fraud to grow exponentially," says Lem.

One method of defending against cyber crime is to develop strong IT systems designed to detect hackers and prevent them from damaging internal infrastructure or stealing data. "In Italy, like elsewhere, there has been a tremendous increase in cyber-attacks," says Pasquale Soccio, Forensic Associate Partner, KPMG in Italy. "In a business world reliant on technology, if a company does not have a robust IT security system to protect against attack, even internal attack, it has a really big problem. A strong IT security system is a prerequisite to doing business." A lot of organizations, however, have been slow to build their defenses. "Many companies fail to develop adequate detection or warning reports to provide alerts on unusual transactions in the system, so it is difficult to detect and track unusual activities," says Rex Chu, Forensic Director at KPMG in Taiwan.

Given that it takes an average of three to five years to detect fraud and that cyber-related crimes are so novel, it may be some time yet before cyber

[8] Stuxnet, for example, is a computer worm discovered as recently as June 2010 that is reported to have been developed by the US and Israel to attack Iran's nuclear facilities.

[9] There is no commonly accepted definition of cyber fraud. Fraudsters have been using computers to help them perpetrate their crimes for decades. This is computer-assisted fraud. Cyber fraud requires a quantum leap in the technological capability of the fraudster, including the ability to decipher heavily encrypted data and break through highly sophisticated computer firewalls.

> Many companies say they have systems in place, but infiltration needs only one or two flaws in the system and years of innovation is lost and stolen by a competitor. You cannot put a price on preventing these lost opportunities.

Alex Plavsic
Head of KPMG Forensic in the UK

fraud has a significant impact on our statistics. "While investigations don't yet show high levels of high-tech fraud or organized cyber crime in offshore markets, global trends make it seem a question of time," says Charles Thresh, Managing Director of KPMG in Bermuda. "We expect to see mobile technology change not only the way fraud is perpetrated, but also how money laundering takes place." This makes it difficult to form a profile of cyber fraudsters. The typical hacker may well be in his/her early twenties, but this may have little bearing on the age of inside fraudsters who are adept at infiltrating computer networks. It may turn out that the average age of cyber fraudsters is lower than for other types of fraudsters. Or we may find that senior managers collude with young hackers working on the outside.

Ostwalt says that "ultimately, the fraudster of tomorrow will depend on the opportunities of the day". Two decades ago, illicitly taking money from, say, a bank was usually accomplished by a closely knit gang, sometimes using violent methods or forged signatures to achieve their ends. The opportunities of today to take money from a bank have been transformed by the internet, smart devices and the ability to analyze vast amounts of data.

In the future, it will still require a group of people operating in concert to commit fraud, but the technological tools will change. A forger is no longer needed in such a group, but a person who can construct a phishing email. A plausible person is no longer needed to present a stolen cheque at a bank teller, but a hacker who can access a protected computer network. Perhaps human features and emotions will no longer be a significant part of the profile; instead, electronic features, signatures and behaviours may be all that a victim organization will know of the cyber fraudster. "To unravel the frauds of the future, the best investigators will be those who are able to reduce large amounts of data to identifiable events with good technology solutions, operating seamlessly across borders and with good corporate intelligence capability to give them quick historical and geographical reach," says Déan Friedman, leader of KPMG's Investigations Network in the Europe, Middle East and Africa region.

The cyber criminal may strike at the heart of the protection taken by organizations and perhaps use those same passwords and encryption techniques to commit the crime. "The key change led by technology is the ease with which intellectual property can now 'walk out' of an organization. Companies do not seem to realize how exposed their systems are to loss of sensitive information," says Niamh Lambe, Director and Head of Forensic for KPMG in Ireland. The environment of computers, the Cloud and the internet makes cyber fraudsters even more elusive than before. This behavior differs from what investigators are used to, and it is something they will have to adapt their methods to. But even cyber crimes are still likely to be driven by the same psychological profiles found previously; only the behavior may have changed. "In the next 3 to 5 years, fraud risk will be affected by the growing reliance on IT and new technologies like mobile payments for every aspect of the business. The old fraud risks will still be around; all we are doing is layering on more areas of risk," says McAuley.

Modern criminal organizations

Cyber crime is likely to become a growing area of interest to criminal organizations; they are already becoming more sophisticated technologically, says Oswalt. He notes that there is a black

market for stolen intellectual property and that criminal groups are involved in it. "Organized crime is getting better at extracting money from corporations. In recent months member firms have seen a rise in payment diversion fraud, where the fraudster relies on new or relatively naive employees to change vendor payment details to divert payments to offshore destinations," says Plavsic.

Cyber fraud would seem to be a logical step. "Organized criminals go about white collar fraud in a slightly different way, using sophisticated technology and placing people in organizations to obtain information and perpetrate fraud. The quintessential internal fraudster is now backed by organized crime," says del Castillo. Unfortunately, the scale of involvement in fraud of all kinds by criminal organizations is hard to gauge, because it is so difficult to detect. Only 15 of the 596 fraudsters colluded with criminal syndicates, 13 of them with both internal and external collaborators. Also, 13 of them involved the misappropriation of assets. Organized criminal groups continue to perpetrate the kidnapping of corporate executives, especially in Latin America and Africa, but there is good reason to believe that in many parts of the world they will extend their reach by engaging in cyber fraud.

The Cyber Crime Underground: A Services Model

Advances in technology coupled with corporate and consumer utilizations e-services are yielding significant gains for the organized and disorganized criminals. Recent crimes around the world illustrate how the traditional bank robbery is evolving into a solely cyber- crime approach, resulting in lower risk, anonymity and significantly greater financial gains. In most instances, organized criminals focus their attention on the utilization of diversified services offered in the cyber underground. Underground services include: botnets for hire (criminal ISP's made of hundreds of thousands of infected machines) enabling users to hide their true identity and to emanate from most any city in the world; malware (malicious software) written for criminals by criminals that are coded to run undetected by virus software and firewalls and focused on stealing identity credentials (such as user name and passwords and credit cards; hackers for hire for specified corporate or device targets; criminal cloud services (bullet proof hosting) leased by criminals for storage of stolen identities or intellectual property; fake webpage's phishing campaigns etc; and money mule and money laundering services.

For financial institutions, bank accounts and credit cards are the main target. In a crime committed in near real-time at multiple locations throughout the world simultaneously, criminals relied upon a combination of unique ATM system knowledge, processes and the technological prowess of the underground outlined above.

The hackers gained access to the bank's databases to compromise 100s of credit cards linked to seemingly legitimate bank accounts. Capitalizing on apparent insider assistance, the hackers were able to gain remote access to a terminal to increase the daily ATM withdrawal limits on each of the cards to more than US$100,000. By exploiting this weakness in the bank's IT security, the hackers essentially created the availability of "fake money" which could then be accessed through appropriated coded magnetic strip cards via ATMs around the world. The final step required the criminal syndicate to use "money mules" to make cash withdrawals from the accounts at more than 100 ATM machines across the world. Within a few hours more than US$45,000,000 was withdrawn unchallenged. As of this writing the true losses are in excess of US$100,000,000. Knowledge of technology and the resources of the organized cyber criminal underground made this global crime possible.

Is this a foretaste of things to come? Yes, and more. Criminals are acting unilaterally and in concert by buying and leasing services of the cyber crime underground enabling less involvement in the criminal chain and increasing ubiquity. Highly competent hackers for hire are likely to be working with leased high-end server farms that have seemingly unlimited computing power. In the near future or now it is likely that "seeker bots", enhanced by self-learning and self-replicating artificial intelligence, will be created to continuously test organizational cyber infrastructure to find the "hole in the fence". On finding a gap, the bots may morph into an "agent" that surveys the landscape of the newly penetrated site to determine the potential for fraud. It may then launch a highly specialized "attack bot", adapted to a victim organization's type and size, infrastructure setup, data volume and other parameters. The bots then may remove assets in hidden or encrypted containers to a single-use, anonymous, virtual delivery location, where the organized crime network can collect the proceeds. The criminal becomes invisible.

Culture of corruption

The impact of national traits on fraud and detection

In some countries, offering gifts is a normal part of business practice, whereas in others it is considered bribery. To a large extent, culture influences our actions and determines what we consider ethical and compliant behavior. Due to different parameters set in different national cultures, a person in China, for example, might have a different understanding of fraud than someone in North America. "Local employees and business partners are bound to have a different perspective on ethics. While gifts and related parties may be fraught with risk elsewhere, for many places in the Asia-Pacific region they are an important part of building a relationship and doing business," says KPMG's Forensic practice in China. Therefore, it is interesting to look at the profile of a fraudster from a cultural perspective. To examine national differences in fraud patterns, we analyzed the results from six countries where 20 or more fraudsters were reported: Germany, the UK, Czech Republic, South Africa, India and Canada.

In general, the variables regarding the profile of fraudsters we investigated were broadly similar across the different countries. Most fraudsters tend to be 36-45 years old in India, Canada, South Africa and Germany, and 46-55 years old in Czech Republic and the UK. The majority of fraudsters in all countries had completed tertiary education and was employed by the victim organization for more than six years, except for Czech Republic where the fraudsters were equally split between fraudsters that were employed between one and four years, four to six years and more than six years. In India, by contrast, the majority of the fraudsters were employed for a period of one to four years. But there were more people committing fraud after working for the victim organization for only one to four years in the UK, Canada, Czech Republic and India, than in South Africa and Germany. This could be due to a higher level of trust awarded to the individual in the first four countries.

The results showed that the most common department where fraud was committed in South Africa, India and Canada was Operations, with large numbers of cases of fraud committed in Finance and Procurement, as well as the Executive office in the UK, Germany and Czech Republic. Similarly, Finance, Operations, and the executive suite were among the three most common departments for fraudsters to work in among the six countries. The level of seniority seems to have a mixed impact on the incidence of fraud. In the UK, Canada, Germany and Czech Republic, the majority of fraudsters were executive directors. There may be less internal checks on directors as they are awarded greater responsibility and trust. In Canada, there was a fairly even distribution of fraud, implying that the level of seniority may not play a large role in the ability to commit fraud, whereas in South Africa and India the majority of fraudsters were in management.

Type of fraud

Within all countries there were more frauds committed with multiple transactions than with single transactions; the latter was selected a maximum of two times per country. Of the six countries Canada was the only country where all the frauds were committed with multiple transactions. Where frauds are committed with multiple transactions the fraudster is more likely to be caught, which could indicate a bias in the results, as once-off transaction fraud may go undiscovered. The time frame for multiple frauds tended to be one to five years within all countries. In this time frame there was an average total cost to the victim organization of US$50,000-$200,000 in all countries except for South Africa, Canada and the UK, where it was higher.

Misappropriation of assets was the most common type of fraud in all countries by a large margin, of which embezzlement, procurement and payroll fraud were frequently employed. Revenue or assets

> Spanish companies should carefully consider possible legislative and fraud risks when entering new markets. Being unaware of how different cultures and business practices affect a company's operations, code of conduct, and legislative responsibilities can be lethal.

Angel Requena
Partner, Head of Fraud Prevention and Detection
KPMG in Spain

gained, fraudulent financial reporting and expenses or liabilities appeared in moderate to large amounts in all countries. Whether the fraudsters were collaborating with others or working alone varied from a 91-9 split in Czech Republic to a 48-52 split in Canada. This implies that fraudsters in Canada, more than in other countries, try to avoid the risks of having an accomplice.

In the majority of the six countries the collaborators were a mixed group, except for the UK and Canada. In the UK the highest number of collaborators were with internal staff whereas in Canada the highest number of collaborators were with external parties. For Germany, UK and South Africa the second highest number of collaborators were with external parties, whereas for Czech Republic and Canada the second highest number of collaborators were with external parties. For Germany, UK and South Africa the second highest number of collaborators were with external parties, whereas for Czech Republic and Canada the second highest number of collaborators was with internal parties. The results showed that for Canada the ratio between internal collaborators and external collaborators were the same. The ratio of all-male, mixed and all female collaborators was also similar across countries except in Germany and India where there were no instances reported of all-female collaborators. In the six countries, the most common motivations were greed and personal financial gain. The results also showed that personal financial difficulty was a common motive for fraud in Canada, Czech Republic and Germany , whereas offenders in India, Czech Republic and South Africa tended to seize an opportunity for fraud rather than planning in advance.

Detection and consequences

In the most frequently cited facilitator of fraud was weak internal control, which was common in all countries. Additionally, reckless dishonesty regardless of controls was most frequently cited in all countries except for Germany. Collusion circumventing good controls was seen as a facilitator of fraud in all six countries except Germany. In all countries, except for in Germany and Canada, there was a significant amount of fraud that was detected through formal whistle-blowing. Germany, Czech Republic, India and Canada did however, have a considerable number of anonymous, informal tip-offs. Other common forms included management review, as well as internal and external audit, which are known as more proactive methods of fraud detection and lead to lower losses as a result.

In general, the consequences of fraud were similar among the six countries with dismissal being the highest reported consequence to the fraudster. Criminal litigation is often avoided by companies that fear the publicity, even though reporting offenders to the police can be a very strong deterrent. In Germany, there was a lower amount of reputational risk to the organization than in the other countries.

Need for nuance

By comparing various aspects of fraud in Czech Republic, Germany, the UK, South Africa, India and Canada, we see that although their national characteristics are similar, there are some significant differences that may be due to variations in culture. As a result, it might be worthwhile for international companies to adapt their fraud risk management programs to conditions in different countries. For example, whistle-blowing may not prove to be effective in cultures where revealing information about others is seen as a negative trait. Similarly, it may prove beneficial to focus deterrence efforts equally between management and staff in India, and more specifically on executive directors in Germany. In the UK, the focus might best be divided equally between the Executive office and Finance. By tailoring anti-fraud efforts to different cultures, organizations might improve their efforts to deter and detect crimes.

Theory of relativity

How the profile of a fraudster is affected by the moral context

In this theme we consider whether the ethical context in which a fraudster commits offences or other misconduct affects the profile of the fraudster. The moral turpitude of the perpetrator of financial and commercial crimes is greater when such criminal acts coincide with, or are facilitated by, bribery and corruption. Bribery and corruption thus has an effect on the fraudster's profile. We asked whether elements of corruption were present in the frauds analyzed in this report and, for 14 percent of the fraudsters who said there was a substantial element of corruption in their responses to this question, we found that bribery and corruption were the offences committed.

When looking globally for environmental factors that would explain the presence of bribery and corruption, we found no clear trend. But when we compared the cases investigated by KPMG member firms in the US, China, the Commonwealth of Independent States (CIS, the former Soviet Union) and West Africa, more definite trends seemed to emerge. In all four countries (or regions in the case of the CIS and West Africa), elements of bribery and corruption in the frauds investigated related to the global average of 33 percent, as follows: the US (24 percent), China (48 percent), CIS (64 percent) and West Africa (67 percent).

Regulation

Our survey was not designed to measure actual moral standards, but instead we asked whether (in the instances of corruption and bribery being present in the frauds observed in the four countries under discussion) the frauds that were tainted by corruption took place in a highly regulated environment. We found that 50 percent of the investigated cases in the US occurred in a highly regulated environment, 50 percent in China, 33 percent in CIS and none in West Africa.

The inverse relationship between the two factors in the table below (the higher the element of corruption in the frauds, the lower the level of regulation) suggests that the institutionalizing of ethical values, incorporated, say, into a regulatory framework, may well affect the profile of a fraudster. This may be the case at least with regard to the propensity towards introducing corruption into fraudulent acts. "Investment is linked to the strength of financial institutions and the quality of governance. Having a company code of conduct to set ethical standards and promote a culture of clean business is not just about fraud deterrence, it's a long-term growth imperative," says Ditty.

	Region				
	Global	US	China	CIS	West Africa
Element of corruption in frauds	33%	24%	48%	64%	67%
Level of regulation	38%	50%	50%	33%	0%

Source: Global profiles of a fraudster, KPMG International, 2013.

Environmental

We then tested the same attribute of the fraudster we observed in the four countries against environmental factors more closely related to the victim organization. We considered the following factors which are known to be sensitive to ethical and moral contexts, corporate competitiveness, market competitiveness and unlimited authority of the fraudster. The results in the chart to the right show the incidence of these three environmental factors in the cases of fraud that included corruption.

The results suggest that there is an inverse relationship between the environment of corporate competitiveness and the prevalence of corruption in the fraudsters' profiles with reference to CIS and West Africa, whereas for the US and China there is a direct relationship. The indicators around an environment of market competitiveness are the same as for corporate competitiveness except for the US where we note an inverse relationship. And there appears to be an inverse relationship between environments of unlimited authority and the prevalence of corrupt propensities in the fraudster's profiles. At a global level, we found that 40 percent of the fraudsters profiled that had introduced elements of corruption in their frauds, had done so in an environment of unlimited authority.

These observations suggest that there are correlations to be found between the behavioural elements of fraudsters' profiles and some environmental factors that can affect the ethical context of the fraudster. However, the links do not seem to be found everywhere and in some countries they may not be present at all. We further considered the cases from a personal, non-environmental, point of view. In this regard we considered whether the fraudsters conveyed a sense of superiority, which is not an environmental factor (see below).

No clear pattern emerges. It seems probable that the sense of superiority is a personal attribute of the fraudsters surveyed, rather than an environmental attribute that could shape the profile itself.

	Region				
	Global	US	China	CIS	West Africa
Corporate competition	23%	25%	43%	33%	25%
Market competition	29%	0%	50%	39%	33%
Aggressive sales environment	31%	25%	43%	28%	8%
Wanting to hide bad news	22%	25%	7%	11%	8%
Unlimited Authority	40%	50%	36%	33%	17%

Source: Global profiles of a fraudster, KPMG International, 2013.

Values and norms

Given the fact that there is no single, unchanging profile of a fraudster, we are skeptical that the trend identified above (between the propensity to introduce corruption into fraudulent actions and the regulated environments observed in the US, China, CIS and West Africa) will consistently stand the test of time.

For now, in some countries, it seems that fraud varies depending on the intensity of the different drivers in time and place. It seems that the impulses created by institutionalized values and norms shape the profile of the fraudster and that the lack of consistency regarding time and place highlights the fluidity of the fraudster's profile.

	Region			
	US	China	CIS	West Africa
Element of corruption in frauds	24%	48%	64%	67%
Sense of superiority	50%	43%	67%	50%

Source: Global profiles of a fraudster, KPMG International, 2013.

Conclusion

There is perhaps a need to emphasize the following key points gained from the insights of KPMG firms' Investigations leaders in the work they have performed and the trends they foresee:

1. Increasing vulnerability to outside threats by "hacktivists" turning their attention to financial gain in conjunction with criminal organizations, armed with technology, seeking both operations disruption and financial gain.
2. The consistent and sustainable upwards trend in collusion between insiders inter se and outsiders which, together with the impact of the point directly above, requires organizations to extend their defending effort against fraudsters' attention and threat beyond the organization's internal control and systems.
3. Corruption and bribery, not a unique event anymore, but more prevalent during the execution of other white collar crimes, becoming a persistent and established part of the contemporary fraudster's profile, improving the ability of fraudsters to create collusive relationships which have a relative higher financial impact on victims than when fraudsters act on their own.
4. Economic instability, volatile capital markets, new technologies and innovation, new accounting systems, increasing connectedness of the world in cyber space and a paperless transactions environment create opportunities for people with the necessary criminal motivation and rationale to apply the required capabilities necessary to gain criminally from these changes.

And while some things will surely change, and we are concerned with the invisibility of the cyber fraudster, one must not forget the typical fraudster may likely remain the tenured, trusted employee. The one you may never have suspected….right in front of your eyes, remaining unnoticed. Forewarned is forearmed.

East Africa

Kenya, Tanzania, Uganda

William Oelofse
Head of Forensic
KPMG in East Africa

- **Reducing tolerance for fraud – reckless fraudsters buck global trends with a quick, large payoff**
- **Untested and unchallenged fraud controls give management a false sense of security**
- **Collusion is endemic – cultural and economic imperative to stay in one job**
- **Enforcement key to reducing opportunities for fraud together with fraud awareness**

There are few hard and fast rules for the profile of the fraudster in East Africa. However, the opportunity for fraudsters is slowly diminishing as consequences increase.

Few rules exist for the profile of the fraudster in East Africa. The myriad of opportunities for fraud at all levels of society and business means multiple faces for fraud and the fraudster. For many of the major frauds, however, the fraudster is internal to the company; senior executives with more opportunity defraud companies of large amounts.

Like fraud, the profile of the fraudster is fluid, adapting to changes in the country, industry, company, or even the individual. Understanding a company's fraud risk requires management to scan the environment, and look more broadly at risk. Context is crucial to understand fraud patterns and anticipate the next threat and face of the fraudster.

Kenya, which is rated the most corrupt country in the region, is a case in point: the environment provides opportunities for the fraudster. Limited transparency and accountability with widespread institutional fraud and corruption engendered a culture of indifference to fraud and the fraudster.

"In recent times, there is decreasing tolerance for fraud as new governments promote freedom of speech and invest in the country's enforcement framework. The attitude towards fraud is changing, from grassroots to business and government; fraud is less acceptable. In short, the window on endemic corruption is slowly closing."

A changing environment has changed the game for the fraudster in Kenya and elsewhere in East Africa. KPMG's African 2012 fraud barometer and the 2012 Transparency International Corruption Perception Index indicate a downward trend in the number of reported fraud cases, although these cases have a higher monetary value.

With these changes, fraudsters have reevaluated their approach, shifting towards a hit-and-run modus operandi, wanting to seize their opportunities before the window closes. Typically, this involves a few transactions to test the waters followed by large transactions over a period after which the fraudster runs or is caught. In a recent banking sector fraud, for example, information technology (IT)-versed employees are alleged to have stolen $18 million from Kenyan banks in one year. This contrasts with the global trend of testing the waters with a few small transactions, and then continuing to defraud the company for three to five years, keeping each transaction small enough to stay under the radar.

"While fraud is prevalent throughout East Africa, it is most evident in Kenya; the surge in development has drawn both people and money to the country, thereby offering a myriad of fraud opportunities, particularly in the financial and government sectors."

In the East African context, collusion is endemic with a small job market and a culture where close relationships are typical. While many companies have controls in place, they are frequently untested and unchallenged, leading to a false sense of security. Long-serving employees of between three and six years continue to feature as fraudsters in the region, having the knowledge to bypass untested controls. In the absence of specific fraud deterrence measures that help combat collusion, companies continue to be exposed to the internal fraudster.

In East Africa, key defenses against fraud are still a work in progress, with East African companies deferring investment until there is a burning issue. Until that moment, fraud happens to other entities.

"Reporting of fraud by employees and third parties is not well established in East Africa; the culture and regulations provide little if no support for the whistle-blower."

Although Kenya is beginning to name and shame, companies mostly still prefer to deal with fraudsters through internal disciplinary procedures rather than legal action.

"Companies are concerned about their reputational risk but are also deterred by the time prosecutions take and the possibility of corruption interfering with the process. How quickly it will change depends on how effective the government's initiatives are to enforce fraud sanctions and set the tone from the top."

The importance of ethics, culture, enforcement, and fraud awareness cannot be overstated in combating the corrosive effect of collusion and the effect of management override on a company's fraud defenses.

Looking forward

Worldwide, fraudsters are expected to continue to innovate and adapt to utilize opportunities offered by new systems and technology.

Cybercrime is increasing in most East African countries. Organizations, particularly banks, face rising levels of electronic crime while fraud awareness from a community perspective is lacking. Governments in the region are also vulnerable to cybercrime as they migrate to paperless environments with controls and fraud deterrents lagging new processes and technology.

"In the next three to five years, we may see the fraudster in the region becoming increasingly sophisticated and senior in the organization as company controls improve, and more fraudsters are successfully tried and sentenced."

Younger generations are feeling a growing pressure to achieve a certain lifestyle, and their ability to utilize technology and social media may well add another face to the fraudster – a younger face.

The pattern of fraud is also expected to change in East Africa; people have to think harder about committing fraud as the opportunity for recklessness is rapidly diminishing while the consequences for fraudsters are slowly increasing.

Unique scenario

Enterprise and entrepreneurship are key aspects of the culture in Kenya and broader East Africa. Many full-time employees run side businesses to fund lifestyles. These businesses usually involve import and export or trading in goods such as vehicles. While these side businesses are not usually used to defraud employers, it does happen. The businesses provide alternative sources of income making it difficult for employers to detect fraud using lifestyle checks. It also creates opportunity and temptation for employees to channel company resources to private businesses and possibly award their businesses company contracts. Poor public databases, and out-of-date company and asset registration creates additional risk for companies dealing with employees with diverse business interests.

In Kenya, communities are relatively small, and in the past, fraudsters sacked by companies or government departments were simply reemployed, with many well-known fraudsters whose cases fail in court being put back into the system. This is improving with strengthening enforcement and local, well-qualified professionals new to the game, many with international exposure, bringing new faces to government departments.

Willie is currently the Partner responsible for KPMG Forensic Services in East Africa. He has been involved in investigations for over 20 years. Willie is a Certified Fraud Examiner and holds an Honours degree in Law from the University of South Africa.

Argentine Republic

Ana Lopez Espinar
Head of Investigations
KPMG in Argentina

- **Competition and clean business challenged by private corruption**
- **Company assets still most threatened by the employee turned fraudster**
- **Collusion key to procurement fraud where external fraudsters are omnipresent**
- **Fraudsters rewarded with termination payments and new jobs**

Our recent KPMG survey showed that almost all companies believed their competitors would violate ethical standards to obtain business.

"Private corruption and collusion, these are the challenges facing clean business in Argentina."

Argentina, Latin America's third largest economy, offers opportunities for local and international business, despite ongoing economic pressures. Yet, business is beset by private corruption permeating its very fabric. No longer the typecast of businessperson bribing government official, corruption is a business strategy to beat the competition and make growth targets.

Countries with austerity measures and predicted impending economic "super derecho" means people and organizations are under pressure and vulnerable to fraud and the temptation to defraud.

Companies see competitors willing to cross the line to win business, and have to make hard decisions in trying economic times. More pressure and little resistance have morphed private corruption into accepted business practice.

"While many companies have codes of conduct and a battery of control tools, they are not regarded as effective. They are formally required policies – something separate to the reality of everyday business."

Corporate ethics are largely driven by top management and the Board through education and sanction; where senior members are aware or involved in corrupt practices, codes of conduct are mere paper tigers.

While the fraud landscape in Argentina is varied, a dominant face does emerge.

"A company in Argentina is usually embezzled by an employee acting alone, although in procurement, we frequently investigate employees colluding with third parties."

KPMG investigations in Argentina show this fraudster most frequently as a male, in his 40s, educated, and in the position for at least two years. Past KPMG surveys have estimated that employee fraud comprises more than 50 percent of fraud in Latin America.

While embezzlement is most often committed by more junior staff, financial statement fraud is linked to management; it is about where the opportunity sits. KPMG investigations in Argentina mirror global findings in that most money is lost from senior management fraud: lower numbers but greater impact.

Financial statement fraud is widespread in Argentina and the Latin Americas, where austerity senior management is under pressure to secure targets. A trend expected to continue, yet the fraudster faces little resistance and few consequences.

KPMG forensic specialists worldwide find companies unwilling to prosecute, fearful of risk and skeptical of their chances of success.

"Companies dismiss employees without taking action; the justice system acts slowly, labor law is complicated, and the process is costly. Fraudsters frequently receive termination benefits on dismissal and move on to other companies where it is business as usual."

Fewer than 35 percent of companies in Argentina had fraud prevention measures at last count, now worsening with back-office cuts.

"Deterring fraud and corruption is hardly top of mind – top management and Boards are dealing with other threats critical to business survival."

According to the Organization of the American States,[1] cybercrime is increasing in the region due to insufficient capacity in cyber security and lack of expertise. The Organization describes a pressing need to "maintain parity with those seeking to exploit digital vulnerabilities."

While the financial sector sees its fair share of cyber attacks on bank accounts, most other sectors frequently see cyber attackers violating data privacy and stealing sensitive information.

"While we see large cases involving cybercrime, these cases are still rare in Argentina compared to embezzlement or financial statement fraud."

Cybercrime has also introduced more faces to the fraudster. Cyber attacks frequently involve an outside person and someone younger.

Preemployment screening and oversight are vital parts of an information technology (IT) security program, as cyber-attackers sometimes collude with internal techies to gain access.

"We are investigating more cases where a company's sensitive information has been stolen with the IT manager or employee playing a role in providing access."

Globally, organized crime is engaging in cybercrime, selling stolen information in underground economies. In Argentina, organized crime has a slightly different persona, less on the fringes of society and more visible. The fraudster seems less an opportunist hit by hard times, than predator – far more deliberate and organized.

Government has signaled a change, introducing additional regulation and setting up a special white-collar crime prosecution unit in late 2012.

"While it is too early to say, the increase in regulation and recent government action to combat economic crime are encouraging signs that the fraudster's life may be shortening."

Looking forward

"Argentina does not have the Asian phenomenon of vast procurement frauds emanating from colossal infrastructure projects."

The fraudster does not seem set to change, except to get younger as fraud turns increasingly high-tech. Fraud does not happen in a vacuum, and as Argentina faces a "fin del ciclo" – the end of a cycle – economic turbulence exposes government and private organizations to many fraudsters.

Ana is a Partner in the Forensic Services practice of KPMG in Argentina, based in the city of Buenos Aires. She joined KPMG's network of firms in 1997 and has over 14 years of professional experience in Forensic Services. Ana is also in charge of Contract Compliance Services as well as Major Project Advisory services.

Ana joined the partnership in 2010, and has served clients in Argentina, Brazil, Bolivia, Chile, the United States, Puerto Rico, Dominican Republic, Uruguay, Perú, Colombia and Venezuela on behalf of Argentinean, European and US entities.

[1] "Latin American and Caribbean Cybersecurity Trends and Government Responses." http://www.oas.org/cyber/documents/OASTrendMicroLAC_ENG.pdf

Australia

Mark Leishman
AsPAC Investigations Leader
KPMG in Australia

- **Understanding how to manage the risk of fraud is crucial and it starts with knowing the risk**
- **Increasing collusion opportunities are enabled by technology and social media**
- **Procurement fraud, misappropriation of cash, and information theft are the most common threats**
- **The employee and third-party contractor feature frequently as the fraudster**

The Australian economy has caused companies to cut costs, and this often starts with back-office and middle management. This will often have a real impact on the effectiveness of companies' internal controls, increasing the opportunity for fraud.

While it is crucial to understand the power of fraud to affect an organization, it is equally important to know how to act, KPMG Australia concluded in its 2012 biennial fraud survey.

Knowing how to act starts with understanding the risk and anticipating where the threat will come from. This is particularly difficult when dealing with the many faces of a fraudster, determined by a myriad of circumstances.

In Australia, frauds committed by employees over 50 years of age are rising, showing people closer to retirement are under more pressure. While greed and lifestyle remain primary motivators for fraud, since the global crisis, KPMG has seen a significant increase in fraudsters motivated by financial pressure as they attempt to maintain high standards of living, or service leveraged lifestyles, in the face of downward pressure on personal incomes and capital gains.

"We increasingly see sharp practices in respect of contracts, with overcharging and liberal interpretation of contracts on the fringes of fraud."

While major frauds are still committed by employees and managers inside the organization, external fraudsters feature significantly in Australia, mostly in respect of credit card fraud and tender fraud.

"The external fraudster appears frequently in the form of the contractor, with project-based work providing opportunity for collusion, bribery, and fraud. Large projects in the construction, energy, oil & gas, and mining sectors all provide opportunities for overcharging and accessing large amounts of money, mostly through procurement – contracts and tenders."

With often rapid growth and isolated operations, companies often have underdeveloped frameworks to manage the risks inherent in their associations with external parties. KPMG encourages

clients to carry out integrity checks with all business partners, including employees, suppliers, and contractors as well as developing processes to monitor their contractor engagement.

As the Australian government moves towards outsourcing models as part of cost cutting, this sector is increasingly exposed to procurement fraud, and other risks that come with third-party relationships, especially if not well vetted.

Australia is a big country, which means that many companies have remote offices. This is also increasing the risk for companies as employees in remote offices under increasing financial pressure have the opportunity to split contracts and circumvent controls or even just misappropriate cash – mirroring a trend seen through Asia Pacific.

In recent times, KPMG has dealt with a number of cases where sensitive government or company information has leaked to the press or customer lists taken and distributed on the Internet. Technology was a key feature not only of these frauds, but also in the KPMG investigation conducted to identify the perpetrator. Cyber crime is also now a worrying feature of Australia's landscape, especially as organizations lag behind in terms of information technology (IT) security as well as general risk assessments of their business processes.

New technology and social media has multiplied opportunities for collusion. While fraudsters still predominantly act alone, collusion internally and with third parties is increasing. This is bad news for companies, as collusion increases the time it takes to detect fraud resulting in bigger losses. With collusion bypassing controls, companies have to look to more sophisticated means of fraud detection, such as forensic data analysis, as well as extending fraud reporting systems to external contractors, in managing their fraud risk.

KPMG's 2012 Australian biennial fraud survey revealed that a number of businesses, although recognizing that fraud is a problem generally, do not see it as a problem for their organization.

"Management frequently regards fraud risk as a single dot on the risk matrix, not always fully appreciating its real nature and extent, which often means it is not then given the attention and treatment required to manage the risk."

The climate for fraud has also generally worsened as companies reduce spending on key internal areas linked to fraud control in trying economic times.

KPMG investigations also reveal that companies expose themselves to fraud by failing to update their internal controls or risk management for new processes, business models, or technology.

Management is a key role player in determining a company's vulnerability to fraud and corruption. Lack of commitment to ethical conduct on the part of senior management has been shown to be a top contributor to bribery and corruption by employees within the organization.

Looking forward

An economy under pressure and an increasing wealth gap is expected to affect the nature and shape of fraud and the fraudster in the future.

"We expect to see more of the older fraudster between 55 and 65 years of age as the economic downturn bites harder."

The internal fraudster and the external contractor are expected to continue to feature in major frauds.

In an environment where fraudsters are constantly adapting to defenses, addressing fraud really requires an appreciation of the threat and some creativity; more innovative and effective fraud measures include job rotation, employment screening for high-risk positions, continuous monitoring, and fraud stress testing.

Unique scenario

"KPMG has helped a number of clients identify the source of sensitive information leaks, providing the necessary evidence to hold these perpetrators accountable. We have done this using our investigation expertise assisted by our forensic technology. Technology is a double-edged sword; technology introduces new opportunities for fraud but it also plays a large part in catching the fraudster. It helps them, but it also helps us."

Mark Leishman is the partner in charge of KPMG's forensic services in Brisbane, Australia, and is also the investigations leader for Australia and Asia Pacific. Mark, a lawyer by qualification, has extensive specialist knowledge of investigations and the fraud and corruption landscape with 21 years' experience in federal law enforcement and 12 years with KPMG throughout Asia Pacific.

Austria

Gert Weidinger
Partner in Charge, Forensic Services
KPMG in Austria

- **Fraud is not the preserve of senior management**
- **More fraud committed against companies by insiders is being detected**
- **Antitrust and corruption legislation is strengthened with more active enforcement**
- **Company proprietary information increasingly vulnerable to cyber attackers**

Antitrust issues are not new to Austria, although the law and environment have seen recent changes. Regulators with stronger enforcement powers are increasingly active; what may not have been investigated a few years ago can now result in huge penalties and fines.

"Fraud occurs at all levels and while there is no single profile of a fraudster, the fraud scheme and damage will differ depending on where the fraudster sits in the organization."

While KPMG often investigates frauds involving management, this does not suggest managers commit more fraud, rather that fraud perpetrated by middle and top management is more damaging for companies and is increasing.

"In the last year, we investigated frauds involving warehouse workers to top management. Higher positioned fraudsters can cause more damage as they can override controls and repeat the fraud for longer."

KPMG investigations reveal increasing financial statement fraud perpetrated by middle to top management, although often acting more as opportunists than predators. When managers cannot get the results they need, many seek alternative avenues to secure numbers and bonuses. It may not start out as fraud, but it is a fine line between financial engineering and fraud and people are not always clear where that line is; having crossed it, they cannot go back, creating pressure to repeat the fraud.

Fraud continues to be perpetrated against companies by top management down to employees, and while not new in Austria, there has been an increase in its detection.

A positive spin-off of the economic crisis has been fraudsters finding it harder to cover losses, as management looks more carefully at a tighter balance sheet.

In competitive markets, companies aggressively seek to reduce or eliminate the competition, and sometimes fall foul of antitrust law.

Technology has been a boon for the antitrust regulator who can now uncover evidence dating back five to six years, placing companies in the difficult position of having to account for decisions made by employees, and possibly former employees, long ago.

"Companies have definitely stepped up on internal regulations relating to competitors, and are training sales staff to have more insight into what is allowed. But we still see areas where the risk is not being managed."

Technical departments, frequently omitted from antitrust training or controls, can unwittingly share competitive information within their small fraternity. Many small to medium-size

companies are also unaware that they may be affected by antitrust legislation following increased thresholds for minor agreements.

Corruption is increasingly in the spotlight in Austria, with frequent reports of management of public companies charged with embezzlement and corruption.

"There is not necessarily more corruption or for that matter increasing corruption, but rather more focus on enforcement and detection driven primarily by the new legislation."

On January 1, 2013, a new anticorruption law came into force in Austria heralding harsher sanctions for bribery of public officials and private corruption, together with an extended jurisdiction incorporating corruption offenses committed by Austrian citizens abroad.

"A decade ago in parts of Europe, companies could deduct bribes in foreign jurisdictions as a useful cost. However, what was previously permitted and considered marketing or a cost of doing business is now illegal; people will need to change their habits – led rather than trailed by legislation."

For most companies, it is still about the bottom line, and with competitors using bribery and corruption to win business, employees need increasingly robust signals from the Board and top executives to maintain the company's ethics and legislative boundaries.

Technology is also affecting the fraud landscape in Austria, with many companies subject to cyber attacks.

"Most of the cyber attacks we see relate to intellectual property and data. We help clients identify how they have been compromised; as the data is still there, it is difficult for clients to know what information has been taken."

One of top management's key challenges is deciding how best to defend against cyber attacks. Securing a physical warehouse is simple with its visible and limited access points; not so for a system where the angle of attack is hard to anticipate.

Weak controls still render companies vulnerable to fraud, with companies overestimating the role of hard controls often bypassed by fraudsters.

"A layered fraud defense affords a company the best protection – a combination of training and fraud awareness, a code of conduct, and a compliance management system."

Rather than deal with all of the governance, risk, and compliance issues in isolation, more Boards are looking at implementing a proper compliance management system.

Looking forward

The question is how fraudsters will adapt and use technology to attack company information and resources in the future.

"This problem is exacerbated with everyone centralizing data in cloud solutions. Managing the risk that comes with these solutions does not stop with the security of the company's information, but also means establishing whether the service provider can be a trusted business partner."

Corruption remains on the agenda in the immediate future. Indications are also that the insider will continue to be the dominant face of the fraudster in Austria in the near future. Even the cyber attacker is commonly seen in KPMG investigations to be an employee or former employee, with knowledge of both what and where to hit.

Gert has been a partner with KPMG since 2005, heading up the Forensic practice in Austria. Gert leads fraud and misconduct investigations and risk management assignments for KPMG. He has experience in business ethics, fraud risk management, as well as internal audit – co- and outsourcing assignments. Gert has acted as engagement partner for several forensic projects with a focus on supporting clients and lawyers in their litigation, eDiscovery, and U.S. litigation cases. In addition, Gert is a certified court expert witness and holds CISA and CIA qualifications.

Bahrain

Arindam Ghosh
Associate Director and Head of Forensic Services, Risk Consulting
KPMG in Bahrain

- **Companies are threatened by migrating management and inactive Boards**
- **Fraudsters benefit from minimal defenses and minimal corporate governance**
- **Endemic collusion and large real estate and construction projects spark widespread procurement fraud**
- **Fraudsters span expats senior manager, senior government official, to junior local employee**

Infrastructure projects and procurement related to the Gulf Cooperation Council's Marshall fund (US$10 billion) will provide many opportunities for the fraudster; the extent to which government and private sector is affected depends on how successful government enforcement is and how much companies invest in corporate governance in the next few years.

Bahrain, a high-income economy, is known as one of the freest markets with a strong private sector. Diversifying from energy, the country has a recognized financial center with banking and financial services, as well as construction and tourism.

This environment offers ample opportunity for fraud, with large energy and construction projects furnishing the fuel for third-party fraudsters as well as bribery and corruption. Recent political unrest in the small island archipelago on the Persian Gulf has fueled a sense of recklessness in some fraudsters.

Against this backdrop and a burgeoning corporate culture, government has focused on initiatives to try and stem the rise of fraud, bribery, and corruption. 2013 saw the penal code strengthened to sanction acceptance and offer of bribes, as well as embezzlement. Legislation extends to bribery and corruption in the private sector and to employees, Board members, and corporate trustees embezzling funds or using their position for personal gain.

With the Bahraini government's strong focus on making the country an investment destination of choice and the business and financial hub of the Middle East by 2030, onlookers expect some active enforcement of the legislation.

"As in other countries, the more serious cases of fraud often involve senior-level people."

Bahrain is a small country characterized by close relationships. In such a close-knit society, organizations face the heightened risk of fraud that accompanies endemic collusion. Many organizations prefer not to risk reputational damage by reporting fraud or pursuing legal action.

Bahrain is cosmopolitan, with many expats working in management positions in local companies. With different ethical norms and business practices melding together, companies in Bahrain are well advised to clarify the boundaries with a company code of conduct, ethical and fraud awareness training for employees and senior management, and sanctioning fraudsters when detected.

"Prosecutions rarely happen, and if expat employees are involved, usually at management level, the consequences are limited to losing jobs and being deported."

In the current political situation, organizations are particularly at risk as people become reckless, abusing weak controls in a last-ditch attempt at enrichment before absconding.

Financial statement fraud is abundant in Bahrain, with managements of privately owned companies embezzling company funds into their own pockets or funding parallel companies and using creative accounting to conceal the gaps.

Managers are often assisted by third-party financial service providers to disguise financial statement fraud, which reinforces the need for critical appointments to be supervised by a Board of directors armed with fraud awareness training. Robust screening of all senior executives and key contractors prior to their appointment helps to prevent this type of abuse.

"A client suspected the company auditor of not doing a good job, only to find he had colluded with the financial controller to disguise financial statement fraud and embezzlement. Critical appointments like financial advisors or auditors are the responsibility of the Board but bolstered by in-depth integrity vetting."

Procurement fraud dominates the fraud landscape in Bahrain, with bids and contract awards contaminated by conflict of interest, rife in this tight-knit society. Opaque procurement processes in both private and government spheres make them more vulnerable to abuse.

"The best defense against procurement and third-party fraud is to ensure you do business with someone you can trust, and then to manage the ongoing fraud and governance risks particularly when subcontracting."

The Bahrain Criminal Investigation Department's cybercrime unit reports increasing awareness has stemmed the tide of cyber attacks; most attacks involve social media, hacking, and cyber fraud gangs offering fake services.

"Cybercrime is definitely happening; outside the financial sector, companies are not detecting or reporting widespread or significant financial losses due to cyber attacks."

While not yet a burning issue for many, cyber attacks are a significant fraud risk. In 2008, a local Bahraini money exchange company discovered an overseas hacker had breached its online security, transferring large amounts of money to personal bank accounts all over the world.[1] However, forthcoming cyber crime legislation may force companies to review their information technology (IT) security and general fraud defenses.

With few multinationals in the country, the corporate governance bar is set by private sector practice. Family businesses are chiefly at risk with minimal controls and fraud awareness.

"We see many public and privately owned companies exposed to fraud, with few defenses. Although internal controls and fraud risk management is not yet embedded in the business culture, the dialogue has started."

Companies will need to review the way they do business and their existing systems and controls, as government leads the way with the Corporate Governance Code of Bahrain coming into effect in early 2011. It may apply to public companies for now, but it is likely to be a matter of time before it extends to private companies.

Looking forward

Unemployment, especially among the young, may herald a younger fraudster, although the profile of the fraudster in Bahrain for now looks set to remain the middle to top manager who is still frequently an expat, senior government official, or more junior local employee. As seen worldwide, the more senior the person, the more damaging the fraud.

Arindam has over 16 years of consulting and forensic experience. He has conducted several investigations for companies in South Asia and the Middle East, helping them detect fraud and take remedial action, including implementation of integrity and compliance programs. Aided by an Advanced Diploma in Computer Application and a Diploma in Electrical Engineering, Arindam has also assisted clients to take a more proactive approach; he has led a number of fraud risk management engagements, conducting fraud and misconduct diagnostics and working with clients on ethics and fraud awareness.

[1] Gulf Daily News August 2013: http://m.gulf-daily-news.com/NewsDetails.aspx?newsid=345409

Belgium

Hilde De Cremer
Director, KPMG Forensic
KPMG in Belgium

- **Common greed still the most important reason for people to commit fraud**
- **Erratic sanctions for fiscal and social fraudsters breeds mistrust for justice system**
- **Ineffective enforcement of regulations does not encourage companies to pursue fraudsters**
- **Internal fraudster protected by privacy laws and strong emphasis on employee rights**
- **Human hacking using social engineering techniques the fraud of the future**
- **Companies are unprepared for intellectual property fraud and theft of information from within**

The regulator strongly focuses on the rights of individuals seeking to 'protect' them from the organizations they work for – an unhappy state of affairs for organizations striving to respond adequately to fraud cases.

International organizations frequently exercise too little oversight of their operations in foreign countries, mostly for as long as the operation is profitable. Local management is given relatively free reign, making these local subsidiaries "easy targets." KPMG investigations in Belgium show local business managers take advantage of this situation, misusing their position of trust and taking decisions motivated more by personal benefit than the interest of the organization.

The Belgium government signaled its intention to focus more seriously on fraud in 2008, appointing a secretary of state to combat fraud and increasing enforcement and sanctions for fiscal and social fraud. Recent cases, however, (e.g., Omega Diamonds NV and massive diamond fraud) illustrate that fiscal and social fraud is treated rather arbitrarily in Belgium, with major tax frauds usually settled amicably with fraudsters not being prosecuted, but smaller cases being subjected to punitive sanctions.

"The penalty tax imposed in amicable settlements of large frauds can be around 30 percent, although an average company that pays for a manager's private trip and does not disclose the benefit can potentially be penalized with the so-called monster tax penalty of 309 percent."

This approach to sanctions erodes the confidence of citizens in the treasury and justice department. Furthermore, because the Belgium regulator is not active in pursuing white-collar criminals, whether internal or external fraudsters, companies frequently choose to simply fire the fraudster or have him or her resign, thereafter strengthening internal controls as needed.

"Perpetrators of insider fraud are not being brought to book or made publicly known. This not only allows them to start over elsewhere, but it also sends the message that internal fraud can pay off."

This situation, combined with strict privacy legislation and the regulation of private investigators, means that employers in Belgium have limited means to investigate potential fraud within their organizations.

The law regulating private investigators has recently been under discussion; by all accounts, if accepted, the draft bill will make investigating allegations of fraud even more difficult for organizations.

For many managers and Boards, the risk of fraud continues to be the problem of other organizations, believing their own employees to be trustworthy and their business environment stable. In Belgium, a number of organizations have therefore given little attention to fraud risk management and fraud deterrence in the past, making the business even more vulnerable to fraudsters.

However, raising fraud awareness through training and fraud risk assessments enables organizations to deter fraudsters and in many cases prevent fraud from happening. But, the success of any antifraud measures ultimately depends on the culture within the organization; setting the right tone at the top is crucial in preventing fraud.

Looking forward

"An increasing number of frauds or attempted frauds are committed using social engineering techniques. We expect this trend to continue in the future, although it is difficult to know how this will affect the profile of the fraudster."

Social engineering is really about manipulating people to carry out certain actions or disclose confidential information; attackers hone in on certain human predisposition (known as "bugs") in an act frequently referred to as human hacking. Techniques include phishing, baiting (where, for example, an attacker leaves an infected USB flash drive near a lift), or cracking identities of people using popular sites.

"Companies are only just starting to get organized to deal with fraud attacks of this nature, and frequently admit that fraudsters are usually one step ahead."

Social engineering fraudsters were generally information technology (IT) specialists in the past, but now specialize in a growing industry, selling tools for "human hacking" over the Internet.

"This is a worrying evolution and companies need to raise the awareness of their employees not only of the threat, but how to protect themselves."

Frequently, companies assume that information security is about technical defenses, forgetting the most important link in the chain – the human element.

"We believe that employees misusing or misappropriating a company's intellectual property or confidential information pose a significant fraud risk in the future."

While companies in Belgium believe that they have managed the risk of intellectual property fraud or information theft, many have only guarded against an external attacker and not the threat from within – the insider.

Hilde is a director within KPMG Advisory with more than 18 years of experience in forensic and related fields, specializing in fraud investigation, contract compliance, internal audit, internal control, and corporate governance. As a certified fraud examiner, and a registered forensic auditor, Hilde also assists clients to understand their fraud risk, and to design and implement effective defenses.

Brazil

Gerónimo Timerman
Head of Forensic
KPMG in Brazil

- **Brazilians drive new "clean company" law and spotlight on rampant government corruption**
- **Combating daily practice of private and government corruption becomes an economic imperative**
- **Possibly new sheriff in wild west of cybercrime with new legislation and growing awareness**
- **No one type of person turns fraudster**
- **Fraudster within the organization uses cybercrime and traditional means**

Brazil has a new focus on integrity which includes anticorruption legislation – already dubbed the 'Clean Company Law.' For the first time, companies are directly liable for bribery, both in Brazil and elsewhere.

Brazil, the world's seventh largest economy, is disadvantaged by the impact of widespread fraud and corruption on public administration and foreign investment. Indeed, public dissatisfaction with rampant government corruption has recently spilled over into ongoing demonstrations and calls for action.

Brazil, ranked 69 of 176 countries in perceived levels of corruption,[1] boasts labels like "*wild west of online fraud*" and "*biggest political corruption scandals in recent history*."

In July 2013, Brazilian lawmakers passed "ground-breaking" antibribery legislation that includes heavy fines and more stringent reporting and compliance programs. The act also touches on fraud in dealings with public organizations and bid rigging. Worldwide, antibribery legislation and active enforcement is forcing companies up the compliance and governance curve. This new legislation is seen as a potential game changer in the corruption and fraud paradigm, set to break the practice of corruption engrained in day-to-day business.

Against this backdrop, it is unsurprising that KPMG investigations show the most common frauds are not related to financial statements, but to the bidding process within procurement, where the lack of transparency frequently veils underlying fraud and corruption.

Typical themes we encounter in our investigations in Brazil are procurement frauds where parties collude, often having a conflict of interest. But the real issue is the lack of transparency in the process."

Another key theme when talking about fraud and corruption in Brazil is cyber crime, with surveys across the Big Four accounting firms reporting at least a third of companies in Brazil now experiencing cyber attacks – higher than elsewhere in the world.

[1] Transparency International Corruption Perceptions Index 2012

"Companies are worried about intellectual property fraud and data theft – a key area for software companies and new media marketing. The illegal market in Brazil for stolen IP and information is big, and new technology makes obtaining these assets easy."

While cyber crime has introduced a new behavior in the fraudster in Brazil, KPMG surveys on data loss pinpoint close to half of digital thieves as insiders, frequently in management positions with opportunity.

Brazil has recently introduced new legislation to combat cybercrime, but the question is whether companies are prepared for this new method of attack or for that matter even the attacks from fraudsters using more traditional means.

"Beyond the well-regulated financial sector in Brazil, I cannot remember seeing a company with a fraud program or fraud risk management. But, if you compare to two to four years ago, the number of companies with internal controls has increased dramatically. Despite a flat economic growth rate, companies are investing in this."

Many companies now have internal audit departments, signaling a big improvement in corporate governance, although still at the lower levels of the control curve. Further up the curve, fraud defenses will need to be within company compliance structures.

As the emphasis on risk management and understanding of risk increases, internal audit departments are edging towards a more risk-based approach, but have yet to incorporate fraud risk properly. The inevitable increased load places a question mark against internal audit departments' capacity, with the new scope and mind-set needing different experience and skills.

Echoing another global trend, KPMG investigations flag contract compliance as a dominant theme in Brazil; as economies tighten, companies are pushing interpretation of contracts to the edge of the envelope.

"Most companies in Brazil are unaware that their contracts are being abused; they have different controls and different licenses for different clients. Controls over contracts are not where they should be, as people more aggressively pursue edgy interpretations."

Contract compliance is really a discussion about fraud risk management; management needs to think like a fraudster to anticipate the soft underbelly of the transaction. Integrity vetting of business partners is a global trend to help organizations preempt the issue by doing business with the right people; in Brazil this discussion is under way.

Many companies in Brazil have a fraud reporting mechanism for employees and third parties like customers and suppliers – a hotline. Brazil's whistle-blowing culture bodes well for the gathering resistance to government corruption and fraud in the country.

"We do not see a type of person turning to fraud in Brazil; it depends on the situation."

KPMG investigations in Brazil pitch the insider as the key threat to organizations, someone in the role a long time, who knows the ropes and the gaps. A person commits a fraud, and if no one is watching, keeps putting his or her hand in the cookie jar. Management positions still offer the most opportunity for fraud; in Brazil, this still means a male, aged 34-plus.

Cybercrime goes beyond the lone hacker; employees and managers are also using their position to commit digital crime, stealing company assets, including intellectual property and sensitive information.

Looking forward

Fraudsters will use technology more and more to perpetrate fraud. Whether corruption continues to stalk business, especially government procurement, depends on how new initiatives are enforced. With clean business an increasing business imperative for foreign investors – under their own regulatory pressure – the fraud landscape is integral to determining Brazil's economic story.

Gerónimo is the Partner in charge of the Forensic practice at KPMG in Brazil and the Head of the LATAM Forensic Competence Center. He has over 20 years of experience both domestic and international conducting investigations and providing fraud risk management advisory services to public and private corporations, as well as national and provincial government entities.

In his Forensic role, he assisted organizations to prevent, detect and respond to fraud and misconduct, conducting investigations, risk assessments and gap analysis; designing and implementing ethics and integrity compliance programs.

Canada

James McAuley
Partner,
Forensic
KPMG in Canada

- **Little increase in financial statement fraud, possibly reflecting the easier economic landscape**
- **Employee turned fraudster with inside knowledge and opportunity still dominant**
- **Data loss and concomitant fraud are top of agenda for Boards**
- **Aggressive enforcement is starting to turn the tide of perception against bribery & corruption and money laundering**
- **A large group of midmarket economy companies still have patchy control environments**

Everyone wants to hear about IT fraud and my answer is usually that IT is often merely a mechanism to facilitate fraud; fraud is committed by people and you need to go back to the basic principles to understand your fraud-related risks.

Canada has fared better than most other countries in the recent economic turmoil, side-stepping many of the issues seen in financial institutions elsewhere.

"We have seen a relatively steady state of fraud in Canada which is partly because of the country's general economic resilience."

However, recent concerns with debt levels and Canada's reliance on global trade suggest possible economic issues moving forward.

"While the fraud landscape has not changed significantly in recent years, companies need to watch the horizon over the next 18 months to see if a changing economy or environment impacts its fraud risk."

In the meantime, the main threat in Canada is still the employee turned fraudster with inside knowledge and opportunity acquired over four or more years in the company – a trusted person.

Insider fraud includes embezzlement, intellectual property theft, and payroll fraud. Bucking global trends, KPMG Canada's investigations do not indicate significant increases in financial statement fraud – possibly a reflection of a comparatively better economic landscape.

Technology is also providing opportunities for fraudsters in Canada. Information technology (IT) is central to daily life and business operations in Canada, providing new opportunities for cybercrime. The financial sector, specifically banks, is currently most affected by cyber attacks; that said, commerce over the Internet creates fraud-related risks. Gaining momentum are the real issues of identity theft and abuse of financial services' networks that affect many sectors.

"There is no question that there are opportunities for people to take advantage of technology, such as mobile payment systems; it's just a matter of how they do this and how these actions will manifest themselves."

More companies in the IT and communication space are moving issues such as the infiltration of their systems, loss of data, and breach of data privacy to the top of the agenda.

Despite technology leading to increased fraud opportunities, check fraud is still a significant risk facing Canadian companies and banks, reminding us that some fraud has been around a long time – check fraud some say dates from the time of the first Persian Empire.

Canadian organizations follow the global pattern of underinvestment in antifraud defenses until required by legislation. Although Canada has been ranked as

a country with a low risk of corruption, companies need to realize that they are exposed to bribery and corruption in their foreign operations due to the impact of Canadian and global anti-corruption laws.

Anti-bribery legislation as well as anti–money laundering laws have been on Canada's books for a long time, but have only been aggressively enforced in the last two years.

"The effects of aggressive enforcement are starting to show. Recent bribery and corruption prosecutions and settlements have turned the tide of getting people to understand that bribery and corruption is unacceptable and will be pursued."

Global companies in Canada have stepped up their focus on bribery and corruption. Where companies have operations in foreign countries, there can be pressure to pay bribes to officials. Different sectors are at diverse points in their antibribery controls and ethos.

"Anti-bribery and corruption regulation is definitely getting more traction, but perhaps too many companies are still not giving it the level of focus it deserves given the risk."

General Counsel ranked bribery and corruption as the least important risk out of nine facing their organizations, in a 2012 KPMG global survey.[1] More important to General Counsel were broader-based risks like regulation and IT, and risk of failure in the supply chain.

"There is still an ongoing perception that the risk of bribery and corruption is not that great, believing it is something that impacts others."

Nevertheless, KPMG is being asked by more clients to help deal with bribery and corruption risks proactively by examining their exposure, both in Canada and elsewhere. On the other hand, companies have generally invested less in antifraud programs in recent years, and weaker enforcement of white-collar crime keeps "traditional" fraud opportunities available for perpetrators.

Overall, Canada has a good control culture, with most large companies having internal audit and strong internal controls, led by the financial sector. However, organizations in Canada's significant midmarket economy will sometimes have a less stringent control culture and a looser governance landscape.

"Many companies think of proactive antifraud measures like insurance – if it may never happen, why spend the money?"

Whether this is a sensible gamble remains to be seen, especially in the face of growing fraud threats and pressure pushing at relatively weak defenses. General Counsel in Canada, and worldwide, believes fraud disputes and fraud litigation to be on the rise.[2]

Looking forward

"In the next three to five years, fraud risk will be impacted by the growing reliance on IT and new technologies, like mobile payments, for every aspect of the business. The old fraud risks will still be around; all we are doing is layering on more areas of risk."

Increasing enforcement of antibribery and corruption legislation as well as anti–money laundering regulations in Canada, and worldwide, is expected to result in more significant issues for companies and increased punitive sanctions.

The fraud threats facing Canadian organizations will be largely influenced in the near term by what happens in Canada's economy in the upcoming year.

Although the inside fraudster has been the dominant threat, this may change in the near future with the latest opportunities for fraud attracting a different profile of people with different skills, possibly people unknown to the company, possibly younger, possibly more organized.

James is a partner in KPMG's Forensic practice based in Toronto. He also serves as senior vice president in KPMG Forensic Inc. He joined KPMG in 1982 and has worked from KPMG's Canada, London, and Toronto offices.

James has more than 25 years of experience with investigations, forensic accounting, and civil litigation. He has been involved with all stages of proceedings including initial assessments, approach, design, research, field work, analysis, reporting, and appearing in civil and criminal court to presenting his opinion and findings as an expert witness. His engagements include assignments in Canada, the United States, the Caribbean, Europe, and Asia. Among other credentials, James is a CPA as well as a certified Specialist in Investigative and Forensic Accounting.

[1] KPMG Survey 2012: KPMG's global study of how General Counsel are turning risk to advantage
[2] KPMG Survey 2012: KPMG's global study of how General Counsel are turning risk to advantage

Central & Eastern Europe

Jimmy Helm
Partner,
KPMG Forensic
KPMG in Central & Eastern Europe

- **Foreign companies vulnerable to fraud as they fail to weigh up local context**
- **Incentive-based pay for local managers of foreign operations drives financial reporting fraud**
- **Asset stripping and embezzlement by local managements of foreign operations a dominant theme**
- **Inside fraudsters less likely to attack homegrown companies**
- **Past practice of collusion, intermediaries, and nepotism drives public procurement fraud**
- **Tight commercial credit means institutional lenders may be more at risk from fraudsters**

With so many different countries, it is difficult to talk about fraud in CEE in broad terms, but in the midst of this diversity, common threads do result in identifiable fraud trends across the region.

KPMG's forensic practice in Central and Eastern Europe (CEE) covers 18 countries, 10 of which are new to the European Union. CEE is the generic term for countries in Central Europe, the Balkans, and Eastern Europe, largely former communist states, each with its own political, socioeconomic, and cultural characteristics, shaping distinctive fraud climates.

Amidst this diversity, there are two common traits that play a noteworthy role in shaping fraud in the region – a shared history of communist occupation and socialist regime, and now the home to operations of many multinational and foreign companies.

"These countries are still shifting from one paradigm to another, from 50 years of communist occupation to independence and participation in a global capitalist market."

Nepotism and favoritism permeated the old system, and continue to operate, through collusion and the use of intermediaries, in the free market capitalist economy. Systems, legislation, and political regimes change overnight, but mind-sets and social norms need more time.

CEE countries are home to subsidiaries, joint ventures, or other remote operations of many multinationals and foreign companies. A recurring theme in CEE investigations is asset stripping, embezzlement, and asset misappropriation by local managements of these foreign subsidiaries and operations.

"Foreign holding companies frequently lack sufficient understanding of the local environment and historical context to properly assess the risk, and manage it appropriately."

While parent companies superimpose codes of conduct onto local operations and boast ethics Web sites, this has not translated into local staff embracing international corporate culture.

Times are changing. While profits flowed in from CEE, parent companies exercised a laissez-faire approach to managing their CEE and other foreign jurisdiction operations, some turning a blind eye to business practices not quite in line with company ethics or codes of conduct.

In the last few years, punitive fines from U.S. anti-bribery regulators prompted a tsunami of regulation in Germany, spilling over into Austria and France. Regulation, stringent enforcement, and dwindling profits has meant management and shareholders are keeping foreign operations on a much tighter rein.

"More foreign companies are increasing local management's incentives linked to performance and cutting formal earnings. We see this triggering increased earnings manipulation and financial statement fraud as managers chase targets."

Multinational companies are changing their approach not only in CEE but also other jurisdictions, like China and the broader Asia Pacific.

"We are working more with our multinational clients in the region, providing integrity training to employees in local operations and assisting with internal audit reviews."

Multinationals are now adapting for local conditions, and investing in layered defenses that encompass soft controls like integrity training and fraud awareness training – not just for the employee but also the director and the Board.

"While multinational companies in the region are investing in fraud risk management, local companies are not."

The fraud picture looks different for local owner-managed business. These companies are less vulnerable to attack by internal employees, with management delegating less and controlling more.

Local business fraud is defined by endemic public procurement fraud led by corruption, and private corruption where business uses bribery to eliminate the competition.

Multinationals have stronger procurement systems driven by regulation, but local business is not similarly constrained.

Building on past practice involving collusion, intermediaries, and nepotism, procurement fraud aided by collusion with third parties and kickbacks is rife in the region. Industries with money to spend and large projects present the most lucrative fraud opportunities, like energy, oil & gas, and construction.

Despite advancing technology, cybercrime, although present, is not yet the dominant fraud risk in the region.

"We see cybercrime and high-tech fraud in technology-intensive sectors like banking, but the majority of organizations in CEE are still typically affected by basic frauds, albeit refined and adapted by the fraudster."

KPMG investigations show traditional frauds taking new twists and turns, with new "opportunities" such as shared service centers being targeted.

Employees and other fraudsters are adding layers to disguise ownership and in so doing, to avoid detection of their conflicts of interest.

"We continue to see the archetypal fraudster in most CEE fraud investigations – a senior executive or manager with authority, and having been with the company for over four years knows the system and its weaknesses. What has changed is more collusion, more recklessness."

The barriers to fraud and related corruption are not very strong or effective in the region. But, the control gaps and fraud defenses vary by country and between multinational and local companies.

"With hard economic times in Europe and CEE, companies are not moving up the defense curve, yet they are more exposed in the current environment with more motivation for fraud."

Consistent with global trends, Boards and managements avoid talking about fraud until it happens; proactive fraud deterrence is not high on the agenda.

"A lot of the organizational risk we see stems from basic things missing from the general environment and enterprise-wide controls."

Unstable politics in the region has also contributed to less effective enforcement as police forces and anticorruption units are repeatedly repackaged and restructured for political gain.

Looking forward

"We expect a significant increase in account manipulation and financial statement fraud. With commercial banks sealing the taps, institutional lenders are going to be prime targets for fraudsters."

With less credit available, companies may engage more in reporting fraud not only to obtain the loan but also to disguise unauthorized usage of the funds.

"While cybercrime will increasingly be a financial sector issue, we do not expect it to dominate other sectors in CEE in the immediate future. For these sectors, we expect it to be business as usual, with opportunists using traditional methods to leverage basic gaps."

Multinationals and foreign companies play a large role in CEE countries; they will continue to do so. More international regulation and enforcement is expected in areas like bribery and corruption, financial statement fraud, and antitrust issues, pushing companies further along the defense curve. While starting with large listed companies, this focus on governance and risk management is likely to cascade down to smaller and medium-size companies. More enforcement and more defenses may prompt a shorter outlook for the fraudster.

For organizations operating in CEE, their response to fraud must be about strengthening the basics first and foremost.

Unique case

Fraud perpetrated in information technology (IT) systems does not always use sophisticated technology: a recent case in CEE related to a company's monthly payroll that had been hacked and the money diverted into another bank account. This was not complex cybercrime; the son of a payroll employee got hold of the password and accessed the server remotely.

Jimmy has led the Forensic practices in CEE since 2000. A former senior advocate at the office of the Attorney-General in South Africa, Jimmy specialized in prosecuting serious fraud cases before joining a forensic practice in 1994.

He has significant experience in fraud and irregularity across multiple industries and jurisdictions. Many of his matters have resulted in successful criminal prosecution, civil action, or disciplinary proceedings with misappropriated assets being traced through cross-border legal action.

Jimmy also specializes in fraud risk management services. He is currently the head of KPMG's Fraud Risk Management services group in Europe, Middle East & Africa.

China

Rachel Layburn
Partner, Head of Investigations
KPMG China

- **Companies continue to underestimate the impact of culture on business practices and risk**
- **Bribery, corruption, procurement fraud, illegal lending, and reporting fraud hit the high notes**
- **The fraudster profile depends on why the fraud takes place**
- **Motivation, opportunity, and justification create the perfect storm for the fraudster**

In China, businesses rely on relationships to get the job done. If the relationship disintegrates, the deal disintegrates regardless of any contract. Internationally, the letter of the law trumps relationships.

China, like anywhere, has a unique culture and an ethical framework that has developed over time. Its culture, however, as in most Asia-Pacific countries, is different from that in North America or Western Europe.

> **"China has its own culture and ethics that companies must understand before they can successfully do business in China, and manage their risk. It ain't like Kansas, because it ain't Kansas."**

China's culture is rooted in a political state, reliant on relationships, politics, and practicalities with a relatively young legal system of some 25 to 30 years. In a society rooted in relationships, legalities and contracts come a distant second.

> **"Against this backdrop, local employees and business partners are bound to have a different perspective on ethics. While gifts and related parties may be fraught with risk elsewhere, for many places in Asia Pacific, they are an important part of building a relationship."**

Multinationals are beginning to fully appreciate the impact of different cultures and life philosophies on how business is done. Having rolled out global policies and procedures on local subsidiaries and joint ventures a few years ago, they are back with version 1.1 – trying to understand how their approach and policies fit into the broader local context and how their employees' ethical framework coheres with cultural and governance requirements.

> **"You can invest in China and bring your business to China, but you need to know China. 110V and 220V both work, but are incompatible. You can't mix voltage, so you need a transformer; it may not work perfectly, but it will work if you are prepared for it."**

Local contracting practices are different from international business. In China, the priority of senior executives is to spend time with business partners socially, developing a bond of trust. The contract is a thin aside, outlining only broad principles, and seldom updated for changes in details.

KPMG frequently helps foreign companies with an eye on China to understand the local legal framework and business practice. While some traditional rules for contract compliance apply in China, such as integrity vetting prospective partners, many do not.

"KPMG worked on a case involving a joint venture (JV) between a foreign entity and a local business. The foreign JV partner sold its share to another foreign company. The local partner, unhappy with the new partner, dismantled the factory moving it and all other assets to another province. Almost overnight, the investment was gone. The relationship had broken down; for the local partner, the share transfer was irrelevant. No time was devoted to obtaining consensus so all was lost."

Bribery and corruption, procurement fraud, illegal lending, and financial statement fraud dominate the fraud landscape in China. While cyber crime is a factor, it is not the priority.

Corruption is problematic in China, penetrating all areas and industries, from high-ranking officials to business and employees. However, as government efforts to reduce bribery and corruption increase, so will enforcement; corruption is perceived to threaten the country's social stability, an area allocated more government funding than national defense.

Describing the fraudster in China is challenging as the profile is primarily determined by why something happens. Anticipating or predicting fraud is therefore about looking at behavior and reasons, rather than particular features of the person.

"People commit fraud when three elements occur simultaneously, the perfect storm; motivation, opportunity, and ability to rationalize the act. In almost all cases, this explains why the fraud occurs and why a particular type of person becomes a fraudster."

In official procurement, the tender process is not sufficiently developed to take into account more qualitative factors of bids, so bidders typically tend to be appointed on price alone. This bidding process is sometimes controlled, not necessarily corruption, but rather procurement trying to appoint the best supplier, not the cheapest. Because the process is not transparent, the regulation gap may also be driving opportunity for misconduct.

Another area of regulation leading to edgy behavior is in the financial sector, specifically extending credit and lending.

"We have seen a significant increase in illegal lending in China. In tough times, companies needing to grow turn to illegal lending to fund transactions."

In China, government controls the flow of money through regulation. Illegal lending starts with noncompliance with what traders believe to be unnecessary and damaging regulation, but fast forwards into fraud as companies fabricate documents and fictitious transactions with related parties to legitimize the flow of money.

While local companies generally do not invest in standard internal controls required by international norms, many not even having internal audit functions, Chinese companies do have their own local defenses to fraud. The power of community means companies rely on the position and power of their senior executives and chairperson to deter fraud or other misconduct. Employees hesitate to commit fraud for fear of sanctions, not just against them but also against their families. They would be unemployable in the tight-knit community.

"Fraud happens in local business, but just as internal controls are meant to deter fraud in the West, so relationships are meant to deter it in China. It is possibly as effective."

For local companies doing business in China, the system works. However, if local Chinese companies want to take business abroad or attract international investment, they need to internationalize their controls and governance.

Looking forward

While more cyber crime is expected, it may not be the next biggest risk.

"Recently, we have seen more senior financial fraudsters, and expect more in the future. While bribery and corruption will remain, we expect more financial statement fraud as the economy flatlines after phenomenal growth – people will find new ways to keep the dream alive."

Chinese companies involved in reverse takeovers are vulnerable to legislative risk and financial statement fraud; for example, a Chinese company setting up a shell company in the United States, transferring its assets to the U.S. entity, but continuing operations in China. They often fail to realize they must adapt local accounting and governance practices to match U.S. or international norms and earnings expectations.

The local senior manager, once founder and owner, is and will continue to be a prominent face of the fraudster in China. This person has enormous practical control over the company.

China is complicated; business is conducted within a political system and based on practical issues. Knowing the legal issues is not enough to do business in China. One must know the market and practicalities.

Rachel is the partner in charge of the KPMG Forensic Services group in Beijing specializing in forensic enquiries and fraud risk reviews. Rachel has gained extensive experience in conducting forensic investigations and compliance risk assessments in mainland China for both multinational corporations and domestic enterprises.

Over the past 14 years, she has led enquiries involving suspected corruption, financial statements manipulation, fund tracing, misappropriation of assets, management fraud, as well as Anti-Money Laundering risk control across various industries in China and North America.

Rachel has led forensic investigations into alleged violations of the FCPA and international anti-bribery laws, financial statement fraud, and kickback schemes. She has advised audit committees, senior corporate officials, and investors regarding corruption prevention and detection, investigative strategies and loss recovery efforts.

Colombia

Latin America

Arturo del Castillo
Managing Director, Forensic
KPMG in Colombia

- **Fraud is growing as fast as the economy**
- **The organized criminal is in the front line in Colombia**
- **Organizations are paying bribes as part of doing business in the private sector**
- **Enforcement of white-collar crime in Colombia is still lagging—25 percent have no fraud defenses**

A concern for all business is that we are about to see a new generation of people, able to use more technology and with access to much more information than past generations – all pointing to a new era for fraud and illegal activities.

Colombia is the land of opportunity for business and for the fraudster. With headlines in recent months like "Is *Colombia the Indonesia of Latin America?*" the country is attracting foreign investment with 4 percent growth and drug-related violence seemingly under control.

A few years ago, companies were small and limited to the local market; these same businesses have now expanded, some exponentially, driven by greater access to local and overseas markets.

Fraud, incorporating financial statement fraud, embezzlement, corruption, and cyber crime, is matching the growing economy, pace for pace.

With so much opportunity for fraud, there is no one profile for the fraudster. The organized criminal is in the front line in Colombia, not only in areas like drug trafficking but also white-collar crime. With organized crime looking to legitimatize cash flows and businesses, money laundering is ever more the order of the day. Recent headlines show financial institutions as a prime target and sometimes coconspirators of organized crime, with names like HSBC, one of the largest banks in the world, being linked to money laundering in Colombia.

Colombian cartels also use financial institutions to make it difficult for investigators to follow the money, sometimes targeting the manager of a legitimate business to negotiate a loan with the institution, instantly creating a credible channel through which to launder money.

"Organized criminals go about white-collar fraud in a slightly different way, using sophisticated technology and placing people in organizations to obtain information and perpetrate fraud – the quintessential internal fraudster now backed by organized crime."

"In some cases, organized crime plants devices to monitor a company's systems and IT defenses to find the way in."

Corruption and bribes are very much part of doing business in Colombia, but with a slight twist. Organizations pay bribes as part of doing business in the private sector – paying to win business, and paying for proprietary information.

Multinational companies operating in Colombia are particularly at risk as local practices may contravene international legislation like the U.S. Foreign Corrupt Practices Act and the UK Bribery Act.

"Where U.S. or UK companies enter into a joint venture with a local company or buy out a local company, they do not always understand the full implications of the local context and adapt their controls accordingly."

The face of fraud in Colombia is not so different to elsewhere. Mirroring global trends, the most frequent attack on companies is still from its own employee with a possible hint of organized crime.

"Banks and regulators are increasingly affected by financial statement fraud, as senior managers manipulate the company's financial information to obtain finance, or even earn bonuses."

KPMG investigations reveal mounting financial statement fraud in Colombia; without changes to governance structures and more consequences for the fraudsters, no respite is expected.

Enforcement of white-collar crime in Colombia is still lagging, as legislation and institutions fall behind the racing economy. Government resources are also stretched maintaining a police presence to manage drug-related violence, the success of which has encouraged foreign investment.

For now, however, little deters organized criminals and fraudsters, and companies are not closing the gaps. KPMG reports fewer than 25 percent of companies operating in Colombia with fraud defenses, with companies also failing to pursue fraudsters in the courts.

Ultimately, the conversation about fraud comes back to why? Another constant worldwide is what drives people to commit fraud.

"It invariably comes down to something that triggers a person to commit fraud – and in Colombia, we find it is mostly the greed of a well-educated fraudster already in a good financial situation."

Looking forward

"Cyber crime and hi-tech fraud will affect more companies and more government institutions. While we have assisted clients defend and investigate cyber attacks, these are not the norm yet. But, they are more frequent and can involve collusion between employees and outside attackers."

With the country recently opened to foreign investment, multinationals are on their way. To succeed, they will need to adapt U.S. or Euro-centric controls and frameworks to the local environment.

Unless Colombia's enforcement regime catches up, the organized criminal will flourish, taking advantage of the new opportunities for private ownership in mining, energy, oil & gas, and telecommunications to legitimize both their money and their business. From drugs to gold is the local catch phrase.

More foreign investment is expected in Colombia, which could see improved white-collar enforcement and corporate governance to build international investor confidence.

With 44 percent of its population under the age of 25, Colombia has a young generation that has access to new technology and social media, and this may herald a new era for fraud and illegal activities.

Unique scenario

The way organized crime uses local business to launder money can be very subtle. A typical transaction has a middleman in a drug cartel providing Colombian businesses with consumer goods for very favorable terms, these orders being filled by goods bought by another person in the United States using proceeds of crime.

Arturo leads and coordinates KPMG's forensic services in Colombia at a national level. Arturo specializes in forensic investigations into white-collar crime and corruption in Latin America, having authored several books and articles in academic journals and decision-maker magazines on the topic.

Arturo has frequently consulted to international organizations, such as the World Bank and Transparency International, on accountability and anticorruption controls, and assisted the Mexican and the Colombian governments with the redesign of national anticorruption policies.

Arturo assists clients with investigations into a wide range of white-collar crimes across a number of industries. He also works with clients on fraud risk management, data analysis, and corporate intelligence.

France

Jean-Marc Lefort:
Partner,
Advisory, Forensic
KPMG in France

- **Procurement fraud colored with corruption a key threat locally and in foreign operations**
- **Stirrings of anticorruption regulators and sense of things to come forces companies onto front foot**
- **French companies turn the spotlight on their exposure to fraud and bribery in foreign operations**
- **Internal controls not interwoven with fraud risk management fail to trip up fraudsters**
- **Senior managers hold all the cards for the big ticket frauds that do real damage**
- **Silence is not golden when monitoring fraud risk in an organization**

We definitely see a change in how companies address fraud, more frequently investigating issues to get a better view of what happened and to build a targeted compliance program.

France has long been associated with international trade, as early as Napoleon III when France and Britain signed a free trade agreement. Today, France is a leading world economy, home to many FORTUNE Global 500 companies and an integral player in international business.

"The fraud environment in France is coming to the boil at the moment, with increasing regulation and companies becoming progressively more aware of the challenges."

When it comes to fraud, KPMG investigations show management and senior executives as the major threat with such positions offering prime opportunity for damaging acts of fraud.

With an economy characterized by industries like construction, nuclear energy, and telecommunication, massive infrastructure projects are always on the cards for French companies, as is procurement fraud tinged with corruption. Government business is a key theme in France, not least as one of the world's biggest exporters of arms – an industry plagued in France by ongoing investigations into kickbacks and corruption. The government is also a business owner, customer, and supplier in the market.

"The majority of our investigations are about procurement and the weaknesses a fraudster exploits in the tender process, the purchase selection, or the contract management. It is the senior manager in a position to falsify tender results or communicate pricing to a friend that really damages a project."

French organizations are starting to concentrate on antibribery and corruption measures, not only locally but also in their foreign operations. This follows escalating enforcement of international anticorruption legislation, and stirrings about impending local legislation and a ramp up in prosecutions. Recently, the Organization for Economic Co-operation and Development's (OECD) report on France's implementation of the OECD antibribery convention[1] focused the spotlight on the dearth of foreign bribery prosecutions in France, and encouraged ongoing momentum in current reforms separating independent investigation and prosecution from political power.

In a slowly recovering economy, French companies still face hard governance choices when competing for contracts both locally and worldwide, especially in high-risk jurisdictions.

"KPMG France assists clients with their problems anywhere in the world; in the last six years, we have done close to 150 investigations for French companies across 38 countries."

[1] OECD: The Working Group on Bribery in International Transactions – Phase 3 Report on implementing the OECD antibribery convention in France, October 2012

KPMG investigations reveal that many companies investing in foreign countries do not always adequately assess and manage the fraud risk of such jurisdictions, or understand their full exposure. Many managements and Boards still treat fraud risk in isolation, missing the overlap with strategic risk.

"Companies are somewhat naïve about the risks associated with certain jurisdictions, skimping on due diligence or failing to ensure appropriate control structures for the level of risk."

But, there are some French companies that are beginning to heed governance risks in their foreign operations, including in Africa, Indonesia, and China.

"In the last 15 to 18 months, companies thinking about ethics and compliance have been calling, especially those that operate internationally. Management wants a better understanding of foreign market risks, together with stronger ethics and compliance programs."

While the majority of companies in France have internal control frameworks, they are not always effective against fraud, bribery, and corruption. Internal controls only become an effective part of a company's fraud arsenal if targeted on risks identified by the company's own fraud risk assessment – remote foreign operations being a case in point. A global trend seen by KPMG worldwide is for companies to send audit or review teams with limited local insight to review local operations.

"We investigated a fraud in a subsidiary company where the local internal audit capacity had been cut, and unfortunately, only one member of the central team could speak the local language."

Although attitudes are changing, the majority of companies remain reluctant to invest in antifraud and antibribery measures unless forced face to face with regulators or fraudsters.

"A company with turnover of Euro 80 billion had four people in its internal audit department. After the fraud, within three years, the company had built the department to 35 people, now having a highly structured business to monitor fraud."

Most organizations in France, as elsewhere, still prefer to keep fraud issues in-house. But, the discussion about fraud is opening up slowly with more companies reporting issues and seeking external independent investigations.

"Companies are more aware that investigations should be conducted in a proper way, preferably independently, and that errors in this process can jeopardize the investigation, the legal process, and ultimately the company's reputation."

Looking forward

"I would be surprised if the profile of the fraudster changes in the immediate future. We expect more big-ticket frauds, and more big procurement issues – the same frauds but aided by highly sophisticated technology."

Local management fraud used to be perpetrated by the fraudster posing as a head office manager either on a call or in a fax to a local treasurer sitting in Africa, requesting an urgent transfer to a new "head office" bank account. Now, the highly technical fraudster can penetrate e-mail addresses and send e-mails purportedly from the head office manager.

Construction, oil & gas, healthcare, and France's military sector will continue to be exposed to threats of fraud and bribery and corruption, with massive international procurement, involvement of governments, and highly politicized transactions.

"We mostly see procurement fraud linked to bribes and kickbacks, rather than pure financial statement fraud. We don't for one moment think this practice will just stop because of new legislation – people will find new schemes."

The fraud landscape in France in the future depends on its continued move towards transparency and independent investigations into fraud and corruption by private and public sector alike, as what grows in the dark usually dies in the light.

Jean-Marc is a partner in KPMG's forensic practice in France. He is a chartered accountant and registered auditor, with 16 years' experience in forensic services. Steeped in investigations worldwide, Jean-Marc provides specific expertise in valuation of damages (breach of contract, counterfeiting, etc.) and provides litigation support to clients and counsel in civil, commercial, and criminal cases. Jean-Marc also assists clients by providing seminars and workshops on fraud and corruption as well as investigation techniques.

Germany

Alexander Geschonneck
Head of Forensic
KPMG in Germany

- **Enforcement is driving the anticorruption culture and controls**
- **The constant threat of corruption requires ongoing vigilance**
- **Antitrust issues are on the increase as companies face a more active regulator**
- **Risk fatigue and isolated fraud risk management weaken defenses against the internal fraudster**

In the wake of recent scandals concerning personal data, companies in Germany are worried about data theft and data abuse. We have seen that in some cases the victims may not be able to detect the particular data-related crime since they lack the overview and the control of the afflicted systems. According to companies, the risk of fraud and economic crime is mostly impacted by human factors instead of e.g. technical or organizational gaps. The typical fraudster is motivated financially or perceives his crime as justified.

In the last decade, Germany has seen its fair share of high-profile fraud and corruption cases, with increased enforcement focusing public and business attention on governance, compliance, and risk, particularly of fraud and corruption.

Even large, well-known companies, such as Siemens, DaimlerChrysler, and Volkswagen, have fallen foul of anticorruption legislation incurring staggering fines, reputational damage, and disrupted operations. All of this has engendered an environment with a strong focus on compliance, with bigger companies investing major time and resources on complying with the checks and balances required by legislation.

"Corruption is no longer the 'one' burning topic; big business feels it has addressed its compliance issues and it's now back to business as usual."

Germany has assumed a "leading position" in the investigation and prosecution of foreign bribery cases.[1] Many companies have chosen to manage their risk of bribery, corruption, and even fraud by using a mix of external legal counsel and internal audit departments, the latter sometimes not having the specialized skills needed for fraud risk management and investigations.

Less overt enforcement in owner-managed businesses, however, means these companies are more exposed to the threat of corruption and sanctions imposed by a very active regulator.

Despite Germany's new status in the anticorruption community, business and government continue to manage the threat, revisiting and adapting systems and controls for new risks from a changing environment.

The focus on anticorruption legislation has not deterred all fraudsters; cartel fraud, rogue trading, mis-selling in banks, other financial sector fraud, and ongoing insider embezzlement continues to flourish.

[1] March 2011 report by the Organisation for Economic Co-operation and Development's (OECD) Working Group on Bribery

"There is a new wave of cartel cases across various industries; this may be the result of new whistle-blowing incentives that offer reporting companies some level of protection from prosecution and potentially enormous fines."

Antitrust law regulators have become more active in Germany and across Europe; the increase in antitrust issues is possibly a question of increased detection.

"Recently, we have worked with companies on antitrust issues, not only providing forensic technology support to the investigation but also assisting management with proactive reviews of their compliance and defense measures."

Antitrust investigations are also fraught with data protection issues, also an increasingly regulated area. Companies in the midst of cartel investigations can find themselves exposed to additional fines and legislative risk if management fails to appreciate the ramifications of data protection legislation, especially when operating across borders.

"We continue to see companies damaged by embezzlement and other frauds committed by an insider in a position of trust. Obviously, technology has entered the arena, but we don't always see who sits behind the cyber attack."

Germany, like many countries, is experiencing elevated theft of company information and intellectual property fraud, a new point of attack against which companies are still formulating a workable strategy. These cases are still widely underdetected and underreported, making it difficult for management to get a real sense of the threat, other than it is there and increasing.

"Companies in Germany have a good attitude towards preventing fraud, but we are seeing an element of risk analysis fatigue due to the increased compliance and regulation demands."

While Boards do well not to overinvest in attempting to eliminate fraud, akin to changing human nature, getting a company's fraud defense line in the right place is crucial.

Fraud risk management continues to lurk on the periphery of risk management, allowing fraudsters to leverage off gaps between processes and departments, with internal audits and management reviews having ring-fenced fraud from other issues.

"More of our clients, especially those that are regulated, are talking to us about integrated systems that can look at their governance, risk, and compliance issues across the organization all together."

Fraud risk, like cancer, attaches itself to any vulnerable part of an organization, irrespective of person, process, or position. Managing fraud risk effectively calls for real integration across business processes and day-to-day dialogue.

Looking forward

The trusted employee or manager will continue to feature in the larger frauds detected and addressed by companies, as long as the opportunity exists. The rise in collusion, however, underscores the need to develop the right culture and ethical environment, as traditional hard controls fail in this situation.

"As a different generation enters the workforce, the question is whether an organization's culture, code of conduct, and risk framework will remain relevant for new ways of thinking and working."

While intellectual property fraud, intrusion into corporate profiles, and other cybercrime seems set to grow, regulators, government, and business are attempting to define and clarify these risks and plot meaningful responses. A new fraudster will emerge, likely an outsider and definitely more elusive. The best defense for any organization will be to keep its information secure and its people aware.

Alexander is a Partner and the Forensic Practice Leader at KPMG in Germany. His focus is on the securing and analysis of digital evidence in the scope of the fight against fraud and corruption as well as the clarification of incidents of IT security and computer crime.

As a recognized expert, Alexander is the author of numerous articles and the German standard book on computer forensic and the correct approach to identifying and analyzing computer-related crime.

Greece

Christian Thomas
Partner, Advisory Head of Transactions & Restructuring, Head of Forensic
KPMG in Greece

- **Subsidiaries of multinational companies have few internal controls inevitably attracting fraudsters**
- **Despite declining corruption due to austerity, public sector still core driver of corrupt practices**
- **Most fraudsters found in Attica Region particularly Athens, drawn by big business and opportunity**
- **Along with bribery and corruption, accounting frauds are the most common frauds in Greece**

Fraud is most common in smaller, family-owned enterprises mainly because they lack the controls to protect themselves against potential fraud – yet these kinds of companies form the core of the Greek economy.

Greece's financial crisis in the last few years has been a crucial factor in the rise of fraud in both the public and private sector. The total cost of corruption in Greece has been estimated at EUR240 million in 2012 and EUR554 million in 2011.

"The public sector in Greece stills remains the core driver of corruption as it continues to receive bribes, with hospitals, tax offices, and construction licensing bodies occupying first place."

However, it seems more recently that while austerity measures may have halted the escalating corruption and fraud in the public sector, financial pressures have seen bribery and fraud continue to increase in the private sector.

The difficult economic climate is forcing companies to cut costs starting with control environments, thereby opening the door to greater exploitation by fraudsters. Further ingredients such as weak internal information technology (IT) controls and little antifraud software have created the perfect recipe for fraud.

The Attica Region sees the highest levels of fraud and corruption (for both public and private sector), particularly the city of Athens. This is because the majority of public services and private sector is based in Athens, as well as 50 percent of the total Greek population.

The most common fraudster in KPMG investigations is a member of the Board of Directors or company's senior management.

Fraudsters in Greece are usually male, which is unsurprising given gender representations in high-level positions.

The profile is 65 percent male versus 35 percent female, between the ages of 35 and 45 years old, and with higher education.

Employees not holding management positions also commit fraud, especially in the finance or sales departments, although these frauds are usually not as damaging to the company.

"The average fraud costs a company between EUR50,000 and EUR200,000 for male fraudsters and EUR50,000 and EUR90,000 for female fraudsters – perhaps not surprisingly given the more senior positions are still held by men."

Typical fraud activities in Greece include bribery and corruption, financial crime

such as falsifying financial statements and reports, and asset misappropriation.

Another factor influencing the increase in fraud is that subsidiaries of multinational companies usually compose a very small portion of the parent company's total revenue, and so holding companies spend limited funds on implementing internal controls – with the inevitable local consequences.

In the private sector, larger organizations and financial services, such as banks and insurance companies, are most likely to be victims of fraud. Fraud in this arena includes manipulation of financial information, unauthorized transfers of funds, money laundering, fraudulent loans, and internal bank frauds.

This means, along with bribery and corruption, accounting frauds are the most common frauds in Greece. Less common but still in evidence are tax evasion and investments frauds.

"For the fraud landscape to change in Greece to any great degree, people and companies need to change their mind-set and culture with respect to fraud."

The implementation of effective legal mechanisms to encourage and protect whistle-blowers, as well as fraud awareness training and ethics training are all measures that can help to change people's outlook, and break embedded tolerance for corrupt practices.

Looking forward

"Due to the economic crisis, people seem to be less accepting and tolerant of fraud, which may help to reduce fraud in the future."

There are signs in Greece that regulators are beginning to adopt stricter measures compared to previous years. This may well tip the risk-reward equation away from the fraudster.

Christian has 13 years of financial, accounting, audit and advisory experience. He currently serves as the Head of Transaction Services & Forensic for KPMG in Greece.

Prior to his current role, he served as Group CFO of Iberdrola Renovables SA in Greece, as well as Audit Manager for PwC in London, UK.

Christian maintains the primary responsibility for overseeing KPMG's Transaction Services & Forensic activities in Greece.

Such role includes providing financial advisory, strategic planning, due diligence, integration, accounting structuring, and transaction-related professional services to KPMG's Transaction Services clients, as well as pro-active and re-active tools and services to assist KPMG's Forensic clients to keep on top of the major risks they face.

Christian's clients include local and international public and privately-held companies.

Hong Kong

Grant Jamieson
Partner in Charge, Forensic Services
KPMG in Hong Kong

- **The employee continues to make use of fraud opportunities within the company**
- **Technology's real fraud risk lies in how management fails to assess its effect on all business areas**
- **Increasing financial statement fraud in hard times as employees do as they are told**
- **While improving, lack of reporting and sanction continues to perpetuate the fraudster**

Although generally a law abiding society, Hong Kong has close family units that extend into the workplace, discouraging whistle-blowing and producing a new kind of collusion. People sometimes help perpetrate a fraud not for any personal benefit but because they are told to.

KPMG investigations reveal that the opportunist inside the company continues to cause damage to Hong Kong companies.

"The type of fraudster we investigate has barely changed; it's still someone who sees an opportunity, has a need, and can justify his or her actions to him or herself. What has changed, however, is the impact of technology on how they both commit and cover up the fraud."

Technology is increasingly used in Hong Kong by fraudsters and cyber-attackers intent on defrauding or damaging companies.

The fraudster still most often seen in KPMG investigations of larger frauds is the educated insider, and often a professional in a trusted position.

"As women start to occupy more of the senior and trusted positions in organizations, we see more women fraudsters."

Recent economic events have inevitably strained compliance and legal resources of large companies already stretched by escalating regulation; the question is whether companies can muster sufficient resources to manage the increasing areas under attack by fraudsters – both internal and external.

Technology is a risk to organizations, not least because management frequently fails to understand the impact of new technology on a company's processes, internal controls, and risk management.

"People see automated systems, such as financial systems, as controls in themselves, believing the lack of people in a process obviates fraud risk."

Furthermore, business in Hong Kong is complex; huge volumes of data and regulatory issues, especially in sectors like pharmaceuticals and financial services, create opportunities for the fraudster.

"Companies have to think harder about whether old fraud prevention technologies still apply. Newer approaches like data analytics and data mining give the company a much better chance of catching the fraudster."

KPMG has also seen more cases of earnings management and financial statement fraud, as harder times and shorter credit lines make it challenging for fraudsters to escape detection.

Ethics of both company and country play a very real role in influencing how fraud is reported and sanctioned. Hong Kong is a well-regulated country with a comprehensive and active regulatory system, an independent commission against corruption, and a high-functioning police force.

However, as in many other countries, companies can tend to keep issues in-house rather than face publicity and reputational risk.

An interesting spin-off from Hong Kong's strong enforcement is that some companies do not invest in fraud deterrence, relying on the police to assist as needed. This reactive strategy can end up more costly than investing in fraud deterrence over the long term. However, while companies in Hong Kong are still more likely to invest in investigations than fraud deterrence, there are signs that managers may be realizing that deterrence can save money.

"Clients have found KPMG staff surveys very useful in identifying current fraud; the process enables employees to consider the implications of their actions and more importantly what they are being asked to do in the workplace."

Looking forward

The drive towards transparency, regulation, and cooperation between countries may lead, counterintuitively, to increased levels of fraud and more fraudsters – not necessarily more fraud but more detection. Legislation, such as the U.S. Dodd-Frank Act, which provides for significant rewards to be paid to whistle-blowers and is applicable to all Securities and Exchange Commission (SEC) registrants, may play a key role in determining how companies react to allegations.

With Hong Kong as one of the freest markets in the world and a gateway to China, Hong Kong will undoubtedly continue to attract opportunists and cyber-attackers.

"The typical fraudster may now be joined by a younger professional just entering the workplace, who thinks about and uses technology in a totally different way to what we have seen before; this will challenge us all."

Companies are now required to rethink controls in light of new technology, and also consider the effect of a new generation on business risk, and corporate culture and ethics.

Unique case

A chief executive officer ran a company for a number of years as his personal fiefdom during which time he embezzled from the company by paying money out of the company's bank account to destinations of his choosing. The clerk making the payments over a period of years explained that he had not asked questions or reported the issue because the chief executive officer was his senior and the boss.

Grant Jamieson is the partner in charge of KPMG's forensic services in Hong Kong as well as China and Asia Pacific. Grant has worked in Hong Kong and China for more than 22 years, and has over 25 years of financial and regulatory related investigation experience. Grant has participated in high-profile financial investigations for the Hong Kong government and other government entities. He has also worked with Global 100 and publicly listed multinationals on financial and regulatory investigations, incorporating preacquisition and pre-IPO fraud, and antibribery and corruption reviews.

India

Jagvinder Brar
Partner, Forensic and Investigations
KPMG in India

- **India has a rapidly and radically transforming macro environment in which corporate entities function.**
- **The penetration of technology increases the dexterity and sophistication of fraudulent acts.**
- **The banking and financial sector continues to be prone to fraud.**
- **Procurement, in both the public and private sectors, remains most vulnerable to fraud.**
- **Cybercrime and intellectual property fraud are expected to rise in the future.**

While India welcomes the much waited Legislation that grants protection to whistleblowers, several obstacles still lie ahead.

Corporate India's new culture of fraudulence

The macro environment in which corporate India functions is rapidly undergoing major transformation. Increased public and media focus on high-profile corruption cases in public procurement contracts, such as the one associated with the Commonwealth Games, the allocation of telecom licenses, and — most recently — the cancellation of mining licenses, has created an awareness in the country regarding widespread corruption and consequent fraud.

India signed the UNCAC in May 2011 and several anti-graft laws have since become effective or are in the parliament.

> **"While India welcomes the much waited Legislation that grants protection to whistle-blowers, several obstacles still lie ahead."**

For the first time in Indian political history, senior political functionaries, including the chief ministers of two Indian provinces, have been convicted of, and sentenced to, corruption, while many big corporate entities are currently facing prosecution. In addition, a new company law, which has stringent provisions regarding frauds, was recently enacted and became effective in April 2014. It has substantially increased the statutory liabilities for corporate fraud. Additionally, a new provision in the Act now makes it compulsory for companies to have independent directors in audit committees. The Act has mandated the company's to report to the Central Government any fraud that comes to their notice during the audit period.

Despite the high degree of focus that fraud and corruption are receiving, a fraud survey conducted by KPMG in India in 2012[1] found that business people were reluctant to discuss bribery and corruption, and the organizational tolerance to them is high. According to the survey, 71 percent of the respondents believed that fraud (of any type) was an inevitable cost of business — implying that fraud mitigation and risk management ranked low on board's agendas. The changing politico-legal factors in the macro environment are bound to affect the attitude of businesspeople in this regard.

[1] KPMG in India Fraud Survey 2012

Another major trend observed is the changing profile of fraudsters in the Indian companies. As a result of enhanced penetration of information technology, the profile of fraudsters is becoming increasingly sohisticated and dexterous. The type of fraud and its degree of sophistication tends to be sectorial in nature. As technology has advanced and has become increasingly easy to access, it gaining popularity as a potential avenue of committing fraud. As a result, certain technology-intensive sectors, such as financial services and IT/ITeS, are more vulnerable to cyber frauds. Relatively older frameworks that were designed to mitigate simple fraud, are now becoming more and more ineffective against refined methods of fraudulence, yet 70 percent of organizations surveyed in the KPMG in India Fraud Survey 2012 had no effective controls or mechanisms to defend themselves against cybercrime or intellectual property fraud and data theft.

"Whistle blowers are often insiders who may have played some role in the corrupt acts."

Technological advancements have made it easier to access a company's intellectual property and data — by either downloading the data on small storage devices or penetrating sophisticated networks. Fraudsters are able to access and cleverly manipulate data in MIS, resulting in MIS-related frauds (internal reporting), such as sales commissions (mainly percentage figures), expenses (forged bills) and assets to ensure that results are consistent with expectations, while still siphoning off money.

Understanding the modus operandi of such frauds and detecting them is not easy; of the respondents of the KPMG in India Fraud Survey 2012, 94 percent agreed that fraud seems to have evolved in the last two years, becoming more refined and discerning. The sophistication of fraud is a new challenge that investigators are grappling with.

"Individuals are more likely to make voluntary disclosures when offered legal immunity and protection which the Whistle Blower Protection Act does not provide."

The broad nature of fraudulent activity continues to be identical to that observed in the KPMG India Fraud Survey 2010.[2] The procurement function and financial functions continue to be most vulnerable. As per the KPMG in India Fraud Survey 2012, the perception of vulnerability to fraud by sector was: financial services (33 percent), information and entertainment (17 percent), industrial markets (14 percent), real estate and infrastructure (14 percent), telecom (10 percent), consumer markets (7 percent) and others (5 percent).

While the perception survey indicates that vendors/agents are most susceptible to committing fraud, as per our experience employees are often the central figure in fraud — they either execute the fraud or assist an external team in doing so. Hence, the larger threat of fraud lies within an organization.

Most organizations tend to ignore or merely warn respective employees when small-value fraud is discovered (such as faking personal bills or fudging expense reports). Therefore, when employees collude with external parties to commit fraud (such as processing fake invoices submitted by vendors), organizations often tend to blame the external parties instead of its employees. This could be a possible reason why the 2012 survey respondents ranked vendors/agents as "the most likely to commit fraud against an organization". Among employees, senior management are considered most susceptible to committing fraud by virtue of their ability to override existing controls.

New variations of frauds (such as intellectual property fraud, data theft, and cyber-facilitated fraud) are likely to create a new profile of fraudsters who are young and work outside the organization.

Jagvinder is a forensic accountant and investigator with 18 years of professional experience, which includes 14 years in the private sector in Canada and India, and four years at the Integrity Vice Presidency, the investigating and prosecuting arm of the World Bank Group. He leads the government, regulatory and other internal investigations practice at KPMG in India.

Jagvinder's experience includes investigations of high profile fraud cases in a public sector bank on behalf of the Department of Financial Services (DFS), Ministry of Finance and the Financial Inclusion Project. His practice includes investigation of banking, procurement and financial statement frauds, embezzlements, corporate frauds including siphoning and diversion of funds, non performing assets, procurement frauds, corruption, collusion, kickbacks and obstruction into investigations. Jagvinder has handled various multi-jurisdictional engagements in a range of sectors including infrastructure, education, financial services, health, mining, retail, service, water and sanitation.

[2] KPMG in India Fraud Survey 2010

Ireland

Niamh Lambe
Director and head
Head of Forensic
KPMG in Ireland

- **Typical fraudster of recent years continues to predominate KPMG investigations**
- **Ireland's tumultuous economy has increased both motivation and opportunity for fraud**
- **Financial pressure sees more financial statement fraud committed by managers under pressure**
- **Mobile technology and increasingly mobile workforce makes company information vulnerable**
- **Sanctions for fraudsters weak as companies reluctant to brave publicity without assured returns**

Having good internal controls is important, but with any control, you are ultimately relying on the human element, which in Ireland is under a lot more pressure. Specific fraud deterrence measures are now even more important to protect companies from losses and reputational damage.

In Ireland, the typical fraudster from recent years continues to feature in the majority of KPMG's financial fraud investigations – the trusted employee. When talking about procurement, you can add external coconspirator to the picture. While this fraudster is expected to remain a threat in the immediate future, there are signs that changes in technology and the workplace may introduce a younger fraudster.

Although Ireland's economy is no longer in free fall, the tumultuous events from the last few years have increased both motivation and opportunity for fraud, a trend expected to continue over the near term. On the other side, with tighter company balance sheets, frauds are having a direct and devastating impact on a business's sustainability.

Since 2008, KPMG has seen an increase in the number of investigations with more financial pressure on individuals and less money being spent on controls and oversight.

"In this environment, it is no surprise that KPMG is doing significantly more investigations of financial statement fraud; senior executives and management are under pressure to artificially improve the appearance of financials and other reports to meet targets and protect the business, their bonuses, and in some cases, their jobs."

In addition, changes in technology and the workplace have created opportunities for fraud, but this is not peculiar to Ireland.

Smartphones, small and powerful storage devices, and mobile payments have introduced new data security risks for organizations. The workplace has also changed with increasing use of BYOD (bring your own device), and telecommuters or nomad workers, making company information even more vulnerable.

KPMG has conducted a number of investigations where individuals left a company for a competitor, were made redundant, or lost their jobs, take sensitive information with them.

These fraudsters are younger professionals familiar with the latest technology, who do not stay with an employer for much more than two years. This new working model exposes companies to new challenges including increased risk of intellectual property fraud and information theft.

"The key change led by technology is the ease with which intellectual property can now 'walk out' of an organization. Companies do not seem to realize how exposed their systems are to loss of sensitive information."

Industries most affected by the recent increase in intellectual property fraud and information theft have been financial services, pharmaceuticals, and construction.

Although sophisticated electronic crime and cyber attacks pose a serious threat to organizations, KPMG's investigations still show the biggest fraud risk to be the internal person with knowledge of the system, the people, and their weaknesses.

Procurement fraud is one of the most frequently encountered frauds in Ireland, and one in which the internal fraudster plays a key role.

What could change the profile of the fraudster may be the increased willingness of companies to investigate and prosecute fraud. Having tighter balance sheets and a lower threshold for loss, companies are investigating both current and historical fraud to recover funds. However, the decision to pursue fraudsters through the courts still depends on the balance between the reputational risk and recovery, rather than a question of deterrence.

KPMG continues to see organizations focus on fraud prevention and deterrence only after the damaging and far-reaching effects of a fraud. However, recently enacted white-collar crime and corruption legislation in Ireland may create more pressure to be proactive.

"Having good internal controls is important, but with any control, you are ultimately relying on the human element, which in Ireland is under a lot more pressure. Specific fraud deterrence measures are even more important for companies to protect themselves from losses and reputational damage."

Corruption can frequently go hand in hand with fraud. However, despite the global perception of increased corruption in Ireland, KPMG has not seen a significant increase in bribery and corruption investigations. In fact, much of Ireland's publicized corruption relates to long-standing corruption of the political process, as well as activities referred to as legal corruption (not yet outlawed by legislation).

Unique scenario

KPMG investigations in Ireland reveal that fraud in high-tech industries like financial services is not always committed using sophisticated technology, but rather using forged and fraudulent documentation. In good times, banks may not have focused on underlying documentation, but now they have tighter controls and are reviewing deals and documents more closely and prosecuting to recover the funds.

Niamh Lambe is a director in charge of KPMG's forensic services in Ireland. She is a fellow of Chartered Accountants Ireland. Niamh has undertaken numerous investigations with a particular focus on regulation and financial services.

Italy

Pasquale Soccio
Associate Partner, Forensic
KPMG in Italy

- **Fraudsters thrive in a business sector under pressure, with few sanctions**
- **Far-reaching international legislation is starting the governance dialogue in local companies**
- **Financial pressure pushes managers into edgy and sharp contract practices**
- **Technology places companies' most valuable asset at risk**

You need to be in a senior position if you are going to bypass controls long enough to commit a fraud that really hurts an organization. Every man supposedly has his price, so deterring fraud in the next few years will be a question of ethics and culture.

Many factors have come together to create favorable conditions for the fraudster. Changes in the economy and the general response to fraud have prolonged the life of the fraudster in Italy.

Weak internal controls in unlisted companies and their reluctance to prosecute have collectively tipped the balance in favor of reward over cost for fraudsters. However, there is a high risk that fraudsters will lose their job.

Frauds perpetrated by employees within the organization have increased. KPMG investigations reveal weak internal controls behind the majority of corporate frauds. Having felt the economic bite in recent years, Italian companies have also cut back on fraud defenses. However, the issue is not simply a question of economics.

"While companies are spending less on controls and fraud risk management because of tighter budgets, most companies do not think they are necessary; there is not yet a strong culture for fraud prevention."

Legislation with international reach, such as the U.S. Foreign Corrupt Practices Act, has without doubt changed the enforcement climate worldwide, and the winds of change are rising.

"Locally, we have seen increased dialogue on compliance and governance prompted by the experiences and actions of Italian subsidiaries of multinationals. However, in Italy, it is still regulation that drives fraud prevention measures."

With the exception of larger listed companies, organizations are reticent about disclosing fraud to the public, worried about their reputation. If they

do disclose, it tends to be driven by legislation. Other factors that can affect management's decision to pursue criminal proceedings are cost and time; the legal process can take up to eight years with no assured outcome.

"Whether companies prosecute depends on their management. We have seen companies prosecute with no recovery possibility to send a strong fraud deterrence message to employees and the market. However, this is not the norm; many companies prefer to just terminate their relationship with the employee."

The economic crisis has not only resulted in cost-cutting but has also affected contracting practice and compliance in the market.

"Recently, we've seen companies acting illegally to save money, with increasing litigation around contract compliance. Whether this will translate into more fraud is yet to be seen."

Sharp practices in contract compliance indicate a business sector under pressure. Pushing boundaries and using edgy practices may not start out as fraud but in the end frequently falls on the wrong side of regulation, and on a tilt of the mirror, an aggressive manager becomes a fraudster. This scenario is becoming all too common with increasingly complex business dealings and managers striving for targets or bonuses.

KPMG finds some companies are unaware they are losing countless Euros as vendors, distributors, and licensees fail to meet contracting obligations. Managing the risks of third-party relationships is more than gaining full value from contracts and intellectual property rights; it is also about deterring fraud and improving business relationships.

A company's intellectual property and information is frequently its most valuable asset. Technology makes company information accessible and vulnerable to theft and manipulation, yet Italian small to medium companies may be ill-prepared for the damage cyber criminals do.

"In Italy, like elsewhere, there has been a tremendous increase in cyber attacks. In a business world reliant on technology, if a company does not have a robust information technology (IT) security system to protect against attack, even internal attack, it has a really big problem. A strong IT security system is a prerequisite to doing business."

Corruption is significant in Italy, with Transparency International rating Italy as the second most corrupt European country. Procurement continues to be contaminated by corruption, with large tenders attracting the attention of organized crime.

The best defense for companies against many of the compliance, fraud, and corruption threats is to know their business partners.

"Many companies are affected by fraud and corruption in their supply chains, involving third parties, tendering, and conflict of interest. While due diligence on the integrity of business partners makes sense, limited public information, outside of the media, about ongoing criminal cases could make it difficult to put this into practice."

Unfortunately, there is limited public information, other than the media, about ongoing criminal proceedings; a final judgment can take up to eight years to get into approved legal registers. Companies therefore need to use multiple sources to build a picture from which anomalies and trends can be spotted. The real secret is to employ this "intelligence approach" throughout rather than once-off prior to contracting.

It goes deeper, however, than local corruption. Many Italian companies investing in other countries find the lack of legislation in different environments challenging, especially where gifts and commissions appear de rigueur, a practice that is then considered criminal by an Italian judge.

KPMG investigations show holding companies should be cautious about positive financial results from foreign subsidiaries which are out of kilter with their economic context; if something is too good to be true, it probably is.

"We also see companies in Italy engaging in financial statement fraud, but this is more connected to fiscal and tax issues as companies try to reduce outflows. The economic crisis may well result in more earnings management frauds being detected in the next few years."

Looking forward

It is never easy to predict the next fraudster, as fraud is fluid and constantly adapts.

While Nietzsche may have wondered whether every man has a price, even he conceded "for every man there exists a bait which he cannot resist swallowing." Companies taking the initiative on preventative measures and creating a top-down ethical environment go a long way to making that bait more elusive and less palatable.

Pasquale Soccio, as associate partner for KPMG Forensic in Italy, is responsible for investigation services. He has conducted a number of investigations, including employee fraud investigations, for local companies and multinationals, providing expert witness in support of Public Prosecutor's criminal investigations. Pasquale also assists clients with fraud deterrence, and is a registered auditor, certified accountant, and certified fraud examiner.

Japan

Goro Araki
Senior Manager,
Forensic
KPMG in Japan

- **Local regulation still not translating into reduction of fraud in Japan**
- **Employees collude because they are told to by their bosses**
- **No one type of fraud, although embezzlement and financial statement fraud dominate**
- **Whistle-blowing unpopular due to Japanese aversion to anonymous reporting**
- **Many Japanese companies at risk as still to implement fraud defenses**

One of the unique trends in Japan is that corporate fraud is often committed to cover past mistakes keeping the respect of colleagues and bosses, and for what is believed to be for the good of the company.

Several high-profile financial statement frauds in the early 2000s put the spotlight on fraud in Japan, prompting implementation of the Japanese version of Sarbanes-Oxley – J-SOX, regulations to improve the reliability of financial reports, compliance with laws, and preservation of company assets. But, this has had mixed success.

"Despite the introduction of J-SOX, we have not seen a decrease in fraud. Currently, regulators are looking at new rules to address this."

White-collar crime statistics in Japan still show the dominant fraudsters as middle to lower rank employees involved in embezzlement and senior managers embroiled in financial statement fraud. The internal fraudster is still the dominant fraudster, someone in the organization long enough to know the systems.

Cyber attacks tend to be carried out by an external person, and while this fraudster does not yet appear that frequently in KPMG investigations, indications are that corporations will see this external fraudster more frequently.

While fraud in Japan is also driven by greed, KPMG investigations often see employees and managers committing fraud for a number of years believing it to be for the company's good, either by manipulating numbers to improve the bottom line or by round-tripping to cover up losses created in the normal course of business.

"We've seen a case where employees tried to hide the company's investment losses, even paying an external adviser to assist. The scheme went on for years until uncovered by a whistle-blower. Other than keeping their jobs, the fraudsters gained little personally."

As elsewhere, Japanese culture influences the country's fraud landscape. In the past, Japan's corporate environment was governed by permanent employment where employees joined organizations on graduation and remained to retirement. Unlike other countries where promotion is often gained by

moving company, in Japan, promotion was a question of tenure. While this trend is still seen in some areas, the job market is opening up.

"Permanent employment engenders a sense of pride and loyalty to the company. Japanese employees' need to serve the company and protect business is greater than elsewhere."

In an environment of permanent employment, employees are more likely to rationalize fraud or bribery that ensures their employer's survival. Work relationships are similar to family relationships as colleagues frequently work with each other for much of their working life.

"We frequently encounter junior employees participating in fraud because they are told to by seniors. With more permanent or lifelong employment in Japan, to stay safe and keep a job, employees often assist bosses perpetrate a fraud even if they feel it is not right."

Occurrences of fraud in Japan are rising, mainly due to an increased sensitivity towards fraud and an increased willingness by companies to deal with the issue.

"From our work especially in the area of audit, we have noticed a heightened awareness of fraud in the Japanese corporate environment in the last few years."

People are more aware of fraud red flags and so are detecting fraud earlier than before. As the job market becomes more fluid, people also become willing to detect and deal with fraud, no longer seeing the organization as a lifelong employer.

"Investigations in Japan are different than in other countries. It's not that executives don't deal with issues, they just prefer to handle them more discreetly until the allegations prove plausible."

Mirroring global trends, Japanese companies concerned about reputational risk rarely prosecute fraudsters, preferring to let the errant employee or manager go. Listed companies in Japan, however, are required to disclose frauds depending on the severity and impact on the financial statements, similar to international accounting requirements.

The control environment and standard of fraud defenses varies company to company in Japan.

"Japan does not have a whistle-blowing culture mainly due to the negative connotations attached to reporting something anonymously. People are hesitant to do this."

Interestingly, KPMG has seen Japanese companies with whistle-blowing mechanisms in local operations frequently fail to implement in their foreign operations, thereby forfeiting earlier fraud detection prospects.

The tendency for organizations to conflate internal controls with fraud risk management is a global trend.

In Japan, while some companies have good compliance programs and a mind-set to deter certain types of fraud, governance structures in Japanese listed companies are still weak regarding the inclusion of independent external parties like the nonexecutive director.

"There is a sense of less risk of corruption in Japan than in other Asian countries. While Japan has the same culture of gifts, government officials in Japan are subject to strict regulation and active enforcement, and regulators and legislation dealing with corruption are relatively strong."

Generally, Japan has a law-abiding culture with one of the lowest crime rates. Japan is ranked in the top 20 least corrupt countries (out of 176 countries).[1]

Bribery and corruption investigations, however, especially of foreign operations, frequently reveal companies with little understanding or sense of deterrence and few controls, making it unsurprising that in the last 6 to 12 months, KPMG has seen rising demand for assistance with antibribery and corruption measures and training for companies, although not for other white-collar fraud and money laundering.

Japan mirrors global trends – investing in fraud deterrence only following a bad experience or when required by regulation.

"In Japan, we generally see management act if it has a sense of heightened risk that a certain type of fraud could occur that would have a strong impact on the company."

KPMG investigations show no particular type or trend of fraud in Japan, but rather fraud taking place where opportunity knocks.

"In Japan, while fraudsters generally act alone, they may have a few external corroborators, mainly because it is very hard to perpetrate large-scale frauds alone."

Looking forward

"Cyber crime is an issue and we expect companies to start looking more seriously at their exposure to cyber-related crimes."

The fraud landscape in Japan may also change as Japan's workforce becomes more fluid. Management may find it harder to persuade employees to collaborate on frauds, and with less loyalty, the risk of lower level staff engaging in fraud may well increase.

Goro Araki is a senior manager in the Forensic practice in Japan. As a CPA and a certified fraud examiner, Goro specializes in cross-border fraud investigation, dispute advisory, and data analytics. He has over 16 years of experience in public accounting including tax and forensic accounting.

Prior to joining KPMG FAS Co., Ltd., Goro spent ten years with KPMG's U.S. practice, including five years in the Forensic practice.

1 Transparency International Corruption Perceptions Index 2012

The Grand Duchy

Sandrine Periot
Director of Forensic Anti-Money Laundering Services
KPMG in Luxembourg

- **Luxembourg steps towards transparency with adoption of charter of quality for private wealth management and removal of bank secrecy**
- **Common fraud reflects global trends of dominant internal fraudster**
- **Employees frequently unaware of consequences of misconduct or of company policy**
- **Luxembourg strengthens antibribery legislation amidst perceived increase in corruption**

In the last three years, there has been further enforcement of existing fraud and corruption legislation in Luxembourg. While organizations are generally aware of the legislation and their related financial and reputational risks, they are still ringing the bell too late when it comes to fraud.

Luxembourg, despite being a small country in Western Europe with a mere half million population, has always been under scrutiny. It is not only the world's last remaining grand duchy and one of the wealthiest countries in the world, but also the largest investment fund center after the United States, with EUR2.4 trillion of net assets under management and the private banking center of the Eurozone.

"The financial sector remains the principal pillar of the economy, attracting massive capital influx. In response, Luxembourg has continued to strengthen its framework in the fight against money laundering and terrorist financing."

Luxembourg benefits from a multicultural and international business-oriented environment backed by a strong regulatory framework and an interesting tax regime that has attracted financial institutions and companies from all over the world.

International debate has gathered around Luxembourg's regulatory framework in recent years, with hotly debated issues of bank secrecy, tax haven status, and transparency.

Some of the recent responses in Luxembourg to face this turbulent environment, and put an end to the inherited but inappropriate label of tax haven, include the adoption of the ICMA's[1] Charter of Quality for private wealth management and the removal of banking secrecy in 2015.

The main principles of the charter are integrity in business relationships as well as transparency towards clients and the regulatory environment.

In the last 10 years, financial institutions have continued to develop strong measures to prevent and detect money laundering and terrorist financing, pressured by both legislation and fear of reputational risk.

In addition, Luxembourg faces the same challenges with respect to fraud as elsewhere.

[1] International Capital Market Association

# of Luxembourg

"Fraud in Luxembourg does not appear to be different from elsewhere in Europe encompassing the same categories: misappropriation of company assets by employees, financial statement fraud, theft, corruption."

There is no specific trend within the market as regards any particular type of fraud occurring more or less frequently.

Although there are few criminal cases reported in the press or the courts, in the absence of official statistics, it is difficult to know whether this reflects a country more resistant to fraud than elsewhere.

Luxembourg is believed to be one of the least corrupt countries, ranked 12 out of 176 countries by Transparency International based on external perceptions.[2]

Nevertheless, a survey[3] published last July by the same organization pointed out that 50 percent of the 502 people interviewed stated that corruption has increased in the past two years. Political parties, business/private sector, and religious bodies are seen as the most affected by corruption.

The country has also amended and strengthened its fraud, antibribery and corruption framework in the last few years by introducing in particular the Criminal Liability of Legal Entities law in March 2010 and protection measures for whistle-blowers in February 2011. This law extends criminal liability for bribery to legal entities as well as natural persons, together with a long arm to pull in offenses committed by nationals in other countries and offenses committed in Luxembourg by foreign organizations.

Luxembourg is undoubtedly a small close-knit community where companies tend not to make details of fraud publicly available. These elements may well increase the risk of collusion and conflicts of interest in business dealings.

"Any organization could face fraud, specifically in this tough economic climate where maintaining earnings and survival are key priorities, but not all of them are well prepared to properly detect and respond to it."

Cyber attacks are also in the spotlight. Recent press headlines highlight the real risk of data theft facing organizations in Luxembourg, especially in its financial sector. Advancing technology is expected to further amplify this threat.

"Organizations need to recognize that fraud can happen and better measure its impact. Most companies are focused on developing their anti–money laundering controls; fewer are focused on fraud risk management, including educating staff and management about fraud and the risks of their particular environment."

Luxembourg's community may also, in a certain way, contribute to prolong the life of the fraudster; wary of reputational damage, companies do not usually pursue the fraudster, preferring to dismiss the employee.

"Management does not always communicate its expectations to employees regarding the company code of conduct, and more importantly, the consequences of contravening it, whether by committing fraud or other breaches of company ethics."

Looking forward

As whistle-blowing plays an essential role in detecting fraud, more fraud may come to the fore courtesy of the new legislation in Luxembourg to protect whistle-blowers. The strengthening of both legislation and enforcement may also drive detection of fraud.

"Companies are waking up to the risk of fraud, but the majority still ring the bell too late; they respond too late to the fraud and the fraud risk. The first step is zero tolerance regarding fraud, starting at the top and filtering down through a code of conduct that management takes the time to explain to employees."

Sandrine Periot has been with KPMG since 1996; she first focused on voluntary liquidations of investment funds, banks, and other financial professionals. She has over 13 years' experience in anti–money laundering services, dispute advisory, and fraud investigations. She frequently assists banks and other financial professionals with compliance function reviews and works with companies in various sectors to understand and manage their fraud risk.

[2] Transparency International Corruption Perceptions Index 2012
[3] Global Corruption Barometer 2013

Malaysia

Sukdev Singh
Executive Director, Forensic
KPMG in Malaysia

- **Developing economy and large infrastructure programs provide opportunity for fraudsters**
- **Frauds frequently involve collaboration between senior internal person and contractor**
- **Companies have a false sense of security as fraud risk prevails where controls are not updated**
- **Misappropriation of assets and basic frauds feature most commonly in Malaysia**

What it always comes back to is that fraud is about people, what they want, and how much resistance they face. This usually comes down to pursuit of a lifestyle, what is culturally acceptable, and the quality of a company's defenses.

Malaysia has been growing at an average annual rate of 5.8 percent for many years; as a consumer-based economy with exports to China, it has been largely resilient to global economic woes. Malaysian banks and companies remain strong, with government still spending significant sums on infrastructure programs, like the US$16 billion MRT Malaysia project.

"Malaysia's developing economy has prompted large infrastructure programs in the last few years, providing many opportunities for the fraudster and giving impetus to fraud."

Escalating levels of procurement, especially by government, and increasing use of third parties has provided much opportunity for fraud. Add to this a long-standing business culture of "middlemen" and lobbying, where related-party transactions are viewed as the norm rather than risky endeavors, and what may be viewed as business as usual would be viewed in other jurisdictions as collusion or corruption.

"Over the last few years, we have seen a number of procurement frauds, which include cost escalation, conflict of interest, flawed tender processes, collusion, and corruption."

Fictitious invoices for work not done where fraudsters collude with subcontractors to fleece companies of assets are common in Malaysia.

"There's almost always collaboration between the subcontractor and an internal person – a manager with authority to appoint a contractor and authorize payment. The internal fraudster will be found in finance, procurement, or sales."

Malaysian companies struggle with relatively few public databases making effective supplier vetting difficult.

Many fraudsters in Malaysia are opportunists and the profile of the fraudster is largely determined by opportunities that arise in the industries in which they work. Currently, the large projects, which include many third parties, in construction, telecommunications, oil & gas, and state-owned entities increase the risk of bribery and corruption.

In addition, Malaysia's fraud landscape has seen an increase in the detection of financial statement frauds.

"In the last four to five years, many more cases of financial statement fraud have been noted, as individuals are motivated to obtain financing to keep their companies alive. There have also been more prosecutions, typically with senior managers being charged with these offenses."

Fraudsters still focus on misappropriation of company assets as companies fail to close the gaps. Asset misappropriation remains the most common type of fraud in Malaysia, including some old favorites such as expense claims, payroll fraud, false invoices, and breach of trust. This fraud has been prevalent in the country for a long time, and shows little sign of abating.

While larger listed companies generally have the controls required by legislation, there is a crucial difference between having a control and implementing it effectively. Many smaller companies are family owned and operate on trust; in the absence of regulatory requirement, they do not see the need to invest in controls until they experience a fraud.

"Most companies think their fraud risk is adequately managed by internal and external audit, seeing no reason for specific fraud risk management. This gives a false sense of security as neither function deals specifically with deterring fraud."

KPMG investigations suggest that employees have often known about a fraud or related issue for up to three or four years, but did not know how or where to report it.

They also show rising numbers of internal opportunists who understand the functionality of the company's information technology (IT) systems, or who collude with members of the IT department to access and manipulate automated systems inappropriately.

As in many other countries, Malaysia's public and private sector are being threatened and targeted by a newer type of fraudster, most frequently an outsider – the cyber attacker. Malaysia's Departments of Defence and Information have both been targeted by hackers in recent years disrupting operations and creating a climate of uncertainty.

"While more companies are investing in IT security, many businesses are still not aware of the extent to which their assets are at risk. IT security, like other internal or fraud controls, is not implemented in smaller organizations in Malaysia."

Companies, however, do seem far more concerned with IT security than general fraud risk management, perceiving an immediate and potential loss from IT intrusions compared to fraud in general. IT security is not just firewalls and sophisticated defenses, but requires integration and some focus on the human element.

Employees and cyber criminals are also targeting companies' intellectual property, with KPMG investigating a number of cases where employees set up competing businesses on the basis of stolen proprietary information. Management of personal devices at work and well-conceived IT policies can be important links in a company's defense.

As fraud keeps pace with the economy, the opportunist and the perpetrator are expected to seek out opportunities in ongoing Malaysian infrastructure and government projects, especially in sectors like oil & gas, construction, and pharmaceuticals for government-owned hospitals. The extent to which Malaysian organizations fall victim to such attacks depends on how quickly they are able to address lagging internal controls, fraud risk management, and IT security.

The dialogue has, however, started with fraud featuring more frequently on agendas at Board meetings and in government, signaling increased opposition to bribery and corruption.

With bribery and corruption being a big concern for government, it has introduced a number of initiatives such as the Whistleblower Protection Act and an independent Anti-Corruption Commission, fashioned on models from Hong Kong and Australia, to address both private and public corruption.

Sukdev Singh, executive director in the Malaysian KPMG Forensic practice, has over 25 years of investigation experience including intelligence, prosecution, and training in criminal and white-collar crimes. Sukdev spent over 13 years in the Royal Malaysia Police as a senior law enforcement officer specializing in white-collar crime. Sukdev holds a bachelor's degree in law and is a certified fraud examiner.

Mexico

Shelley M. Hayes
National Partner in Charge, Forensic
KPMG in Mexico

- **Inside asset misappropriation and procurement fraud dominate Mexico's fraud landscape**
- **An older employee with longer tenure in the organization becomes the typical fraudster**
- **Companies wary of the legal system and impunity for offenders do not pursue fraudsters to the fullest extent possible**
- **Senior managers use shell companies to strip assets or facilitate tax fraud**

The challenges facing Mexican companies are not insignificant. Focusing on fraud mitigation measures, and the allocation of resources, needs to compete with, among others, significant issues in the country related to security and corruption.

Mexico is not only one of the largest nations in the world but also one of the most populous Spanish-speaking countries in Latin America. It is across this dense country that fraudsters appear to be winning many of the battles.

KPMG investigations most frequently encounter fraud in Mexico in the form of asset misappropriation by trusted inside employees, acting alone or in concert with third parties. Companies are attacked much less frequently by external fraudsters. In Mexico, there is less financial statement fraud and earnings manipulation than in countries with greater numbers of listed companies.

"What has changed is that we are seeing a slightly different fraudster. Previously, the fraudster was younger, between 25 and 30 years of age with less time spent with the company. Now, we are seeing the dominant fraudster being 30 to 40 years of age with 3 to 10 years' experience in the company."

This fraudster is a more dangerous profile for companies; with increased access to systems, knowledge of control weaknesses, and long-standing relationships, this fraudster wreaks more damage on companies. Many fraudsters also escape unscathed as few companies in Mexico seem inclined to pursue criminal proceedings by taking a fraudster to court. Not only do matters take a long time to push through the legal system, but this system is also perceived to offer impunity for offenders; case after case of suspected fraud and abuse by politicians appear in the public spotlight, but few indictments follow.

"Companies frequently perceive the costs of pursuing a fraudster to outweigh the benefits. Legal costs, time, and the suspicion of being a target for solicitation of additional extra-official payments to ensure a fair trial discourage companies from taking legal action. However, we find companies often undervalue the strength of a well-prepared case, supported with evidence, not to mention the other benefits in this decision, such as sending a message of zero tolerance for fraud to employees and business partners."

A dominant theme in Mexico's fraud landscape is procurement fraud, which includes schemes where vendors (suppliers) collude with employees to secure work, inflating prices to provide the employee with a kickback, or in some cases, blatantly setting up shell companies that don't provide any type of services or goods.

Although statistics indicate that fraud, mostly theft, is most frequently perpetrated by employees in low- to mid-level operational roles, these frauds are often investigated in-house—that is, by the company. KPMG generally assists clients with issues relating to higher profile fraudsters—CEOs, CFOs, former owners or shareholders, and commercial directors to name a few.

"We frequently see senior management members setting up 'phantom' entities to issue invoices to their employer for the provision of nonexistent services. These shell companies are also set up to sell 'legitimate' invoices to companies for services not provided, but which can be used by the buyer to claim fraudulent tax deductions."

The phantom or shell entity is also at times used by companies to siphon money out of the company in order to fund corruption payments.

Like elsewhere, cyber attacks are starting to appear more frequently in Mexico. For the moment, these attacks are mostly in the financial sector. Currently, the cyber attacker is mostly an external party—a stranger to the organization. Along with companies worldwide, the preparedness of Mexican organizations to address these types of attacks is questionable.

"The fraud we see in Mexico is generally fraud or theft for individual or personal benefit; it is not the same issue as corruption or competition issues that have the potential to impact a much larger part of the population. Curbing fraud will take concerted individual effort by each company to implement appropriate controls and, more importantly, antifraud measures like fraud awareness and ethics training."

Looking forward

"Currently, we do not expect fraud, or the profile of the fraudster, in Mexico to change significantly in the medium term. The extent to which companies will suffer losses from fraud will depend on how quickly companies respond to changing business environments and invest in appropriate fraud deterrence measures."

Shelley is the national partner in charge for the KPMG Mexico Forensic practice, based in Mexico City. She has been with KPMG since September 1993 working in many of the firm's offices including in Canada, Belgium, the United States, and Mexico. Working in Mexico since September 1999, Shelley primarily provides forensic services related to fraud and corruption investigations and advisory in commercial disputes throughout Mexico and Latin America.

Shelley has authored and coauthored various articles and publications, and is frequently invited to speak at national and international events.

Netherlands

Yvonne Vlasman
Partner, Forensic
Lead of Investigations and
Dispute Advisory Services team
KPMG in the Netherlands

- **Tough times and little tolerance for mistakes engenders accounting and financial statement fraud**
- **Companies batten down the hatches with good internal controls, but are short on fraud defenses**
- **Procurement fraud stalks business, especially if vulnerable to kick-backs and conflict of interest**
- **Despite public and media intolerance for fraud, companies still reluctant to pursue fraudsters**
- **Neglected red flags, siloed risk management, and insider knowledge allow frauds to go undetected**

Organizations, especially in the public sector, no longer have the luxury of ignoring red flags. Before the tendency was to underreact; now organizations sometimes overreact, even before investigating the reasons for the red flag.

"The increase in fraud cases we see in the Netherlands doesn't necessarily mean more fraud; rather, more cases are coming to light earlier. There is more detection."

With little tolerance for fraud, the Dutch public and media attention drive transparency, making it harder for companies and government to deal with issues in-house. Fraudsters, however, continue to evade sanction as companies wary of reputational risk prefer to settle the issue and dismiss the employee.

However, some credit for the increased detection of fraud must be given to improving internal control environments found in companies and government institutions. On the downside, recent economic pressure has meant companies having to reshuffle priorities and restructure, leaving fewer people in internal control functions – the risk being that prior gains may reverse.

While the Dutch financial sector has always been ahead of the internal control curve, aided by regulation, government, education, and healthcare sectors have recently made up lost ground, now exhibiting strengthened controls. In general, though, Dutch companies have battened down the hatches, secured by governance and internal control frameworks firmly in place.

"The thing about fraud is that it is an intentional act seeking to bypass an organization's internal controls. This means you have to watch for signs that warn of a breach in controls and then act on them."

Managers and internal audit have started to pick up on warning signs, but there is some way to go. KPMG fraud investigations still show neglected red flags and insider knowledge about a fraud for months if not years before the fraud is detected.

The economic downturn has inevitably increased the risk of fraud in the Netherlands as personal finances and impending corporate bankruptcies place people under pressure.

"With the economic pressures, several companies facing bankruptcy and unable to meet stringent targets and ratios set by financial institutions have been resorting to financial statement fraud or earnings manipulation to demonstrate growth."

In an environment with less fat on the bone, what may have passed unnoticed three to four years ago is now being detected. There are also fewer options for concealing or offsetting losses caused by judgment errors and bad investment decisions with other business gains. With diminished tolerance for mistakes, senior managers are resorting to accounting and financial statement fraud.

KPMG investigations show certain obvious red flags increase the risk of accounting-related fraud, which if present, justify more vigilance from auditors and the Board; these include remote operations, a business unit in a foreign country, or a unit with a very different business making translation difficult for head office.

"We see a variety of people involved in financial statement fraud from members of the Board of directors, the management of a subsidiary, to the financial controller. The best defense is not to believe everything you see. If something is too good to be true, it probably is."

Procurement fraud continues to be an issue both in private and public sectors, particularly driven by conflicts of interest. While all industries are vulnerable, government and healthcare are particularly at risk with frauds going hand in glove with kickbacks to officials, and government doctors.

"We have also seen an increase in fraud not at management level but below, where employees see an opportunity to gain extra income – not thousands or millions – by manipulating, for example, their expense claims."

Motivation and opportunity is picking up more rapidly than fraud deterrence and defenses; while internal controls are good, they are not effective in deterring fraud. While organizations in the Netherlands do not have the budget for comprehensive fraud deterrence measures, many have implemented fraud reporting lines in sync with the recent European focus on whistle-blowing as an anti corruption measure.

"We have dealt with more women whistle-blowers in recent investigations than in the past. With the trend in Europe for internal and external fraud reporting, Boards have to deal with many more allegations."

While larger companies in the Netherlands have started to recognize the parameters of their exposure to fraud, smaller family-owned companies continue to be at risk, still believing fraud happens to someone else.

KPMG investigations reveal many companies still deal with fraud in isolation, resulting in gaps and risks going unnoticed, with some companies even ignoring the risk and favoring a system of trust.

"We most frequently see a company's fraud risk managed by the financial controller or in bigger companies by a separate fraud department. We have not come across a lot of organizations that have integrated their fraud risk management across HR, operations, and finance, or where there is active involvement by the Board."

Looking forward

The increased pressure to commit fraud is not expected to dissipate in the Netherlands as the effects of the economic crisis continue. The Netherlands also faces the worldwide threat of cybercrime and other related high-tech frauds as professionals increasingly use sophisticated technology in their daily work.

"The worrying thing about cyber attacks and high-tech fraud is that it is so easy for perpetrators to gain access; many companies don't even know it is happening."

Traditional frauds and the traditional fraudster will dictate the fraud landscape in the near future, albeit using varying and definitely more high-tech means. The profile of the fraudster will continue to be dictated by opportunity; KPMG investigations show more women fraudsters appearing as more of them move into management positions and encounter more opportunities for fraud.

Yvonne leads the KPMG investigation service in the Netherlands and has over 20 years' experience as a qualified accountant and forensic investigator, specializing in financial and economic crime and litigation support relating to criminal proceedings. Yvonne has performed many fraud risk management projects and frequently facilitates training programs around compliance and integrity awareness, having a post master's qualification in forensic audit and integrity management.

Norway

Per A. Sundbye
Partner, Advisory,
National Head of Forensic
KPMG in Norway

- **More fraud detected with greater general awareness, better systems, and more employee reporting**
- **In a trust-based, conflict-averse culture, companies often shy away from pursuing fraudsters**
- **Nepotism and cronyism common colors of corruption in Norway**
- **Increasingly cosmopolitan, companies must adjust controls for cultural and ethical diversity**
- **Growing privacy rights make it more difficult for companies to investigate fraud**

It has become more important for local companies to manage the risks of new business partners as they are increasingly held accountable for the actions of business partners, not only agents and intermediaries on the revenue side but also partners on the supplier side. Bad reputation and adverse events are highly contagious.

Norway, situated in Scandinavian Northern Europe and known for its environmental focus, is among the world's richest countries. With oil revenues preserving the fiscal balance, Norway remained relatively unscathed in the recent global economic crisis. Even against this backdrop, however, the same fraud and corruption occurs here as elsewhere.

"There will always be the typical type of fraud in Norway – embezzlement by employees and management fraud."

More fraud does however appear to be detected in Norway than ten years ago.

"We have seen an increase in reported fraud cases although it doesn't necessarily mean there is more fraud. Companies have better systems and better communication channels so employees are more aware of when and where to report their suspicions. Ten years ago, this was not an issue; it was hardly talked about, not in the press not inside the organizations."

Norway's small community culture also affects the fraud landscape, quietly influencing how society and organizations address and respond to white-collar crime and corruption.

"Norway is a small close-knit community and has therefore developed a trust-based society that is generally conflict averse – similar to other Scandinavian countries."

Organizations in Norway rarely report fraud; like most businesses worldwide, local organizations fear reputational damage and in Norway, companies have no legal obligation to report white-collar crime to authorities.

"It is uncommon in Norway for organizations to report fraud to the police. The focus is on recovering funds using civil remedies, or more often off-record settlements or compromise agreements, rather than criminal proceedings."

While there is too little information to build a trend, a focus on third-party risk is growing, with an increasing spotlight on risks associated with joint venture partners, suppliers, and other third parties.

Society and regulators are holding companies increasingly accountable for supply chain integrity, from health and safety, environmental issues, and human rights to bribery and corruption.

KPMG investigations reveal Norwegian companies rarely having adequate controls and processes to manage third-party or business partner risk effectively, exposing local companies to financial and reputational losses when operating in foreign jurisdictions or with foreign business partners.

"Organizations need to use comprehensive and reliable business intelligence to get to know their business partners, and ensure that they have real control and influence in the business."

Organizations within Norway are also dealing with an increasingly cosmopolitan society, adjusting traditional trust-based control frameworks to cater for the risks associated with diverse cultural and ethical mind-sets.

In recent years, KPMG has also seen the entrepreneur who having sold control of his company to another investor, continues to treat the company and its asset as his personal fiefdom, resulting not only in tax implications but also representing embezzlement.

Despite ranking in the top ten least corrupt countries in the world,[1] bribery and corruption occurs more often than people would expect. Corruption in Norway does not always entail a flow of cash or assets between parties, being more frequently characterized by an exchange of favors or influence. While there are instances of corruption accompanied by simple and immediate financial benefit, influence seems to be an equally tradable commodity.

A recent Transparency International survey in Norway revealed that political parties and business were least trusted by those surveyed when it came to corruption, although confidence in enforcement structures remained high.[2]

"The tone from the top cannot be overestimated when setting ethical standards. It is harder to combat issues when ordinary people observe or believe that 'important' people, even leading politicians, practice this type of behavior."

While Norway has seen few prosecutions of local companies in terms of foreign legislation like the U.S. Foreign Corrupt Practices Act or the UK Bribery Act, local prosecutions relating to bribery and corruption do happen. Norway has its own antibribery and corruption legislation based on European blueprints with local modification and is quite vigorously enforced.

While some companies have effective antibribery and corruption controls, and deterrence measures, it is by no means the norm. Companies that have experienced a fraud, or been through a bribery and corruption case, tend to have good controls, having turned things around and significantly improved their systems. However, change is evident; KPMG now assists companies almost as much with fraud risk management as with investigations – the turnaround is significant.

1 Transparency International Corruption Perceptions Index 2012
2 Transparency International Norway report, Helge Renå, June 2012, "The Norwegian integrity system – not entirely perfect?"

Top management and Boards of directors are more aware of their responsibilities and liability with respect to governance, compliance, and risk, including their responsibility to manage the risk of fraud, bribery, and corruption.

"While fraud is on the Board's agenda, the level of oversight does vary. Boards may ensure they receive written confirmation from management on sufficiency of controls and systems to manage risk, but their primary focus is business development. It is easy for directors to assume that management has issues like compliance and combating fraud under control."

Although there is more awareness of fraud and corruption, KPMG investigations show that there is still room for more action on the part of top executives, management, and audit committees. Frequently, reporting lines and communication channels are the reason for insufficient Board oversight of key governance and compliance issues.

The typical profile of the fraudster in Norway, however, continues to be the male, in a management position who has been with the organization long enough to know where and when to take advantage of the system.

"In Norway, our investigations reveal top management as the typical fraudster. We don't often see Board members involved in frauds."

Looking forward

"With increasing globalization, companies need to fully understand the environment they work in abroad."

With more competition for resources expected, third-party risk is expected to pose significant risk to Norwegian organizations operating abroad, including government.

"We also expect the more international environment 'at home' will challenge the policies and control structures of local companies as they adapt to incorporate the changing norms and risks associated with different mind-sets and cultures."

The intensifying focus on data privacy in Norway, as in the rest of Europe, will make it harder for companies to employ effective monitoring activities and investigate suspicions or allegations of fraud by employees and management. This creates opportunities that are exploited by the culprits, and fosters the perception that fraudsters are afforded more protection than the actual victims of fraud. The best defense for companies is to know the regulations, and implement proactive processes within the law that afford them some protection.

While technology will appear more frequently in white-collar frauds, cyber crime has so far been dominated by the third party – the stranger outside of the organization.

Per A. Sundbye has close to 20 years of auditing and consulting experience and is an expert in special investigations, litigation support, and fraud prevention and awareness. He has spent more than 15 years outside of his native Norway, and worked on projects in over 35 different countries. He has worked on a large number of high-profile and international investigations across Europe covering areas such as fraud, embezzlement, asset tracing, market abuse, and reviews related to foreign corrupt practices and money laundering regulations. Per holds an MS degree in business and is a Certified Fraud Examiner.

Qatar

Arindam Ghosh
Associate Director and
Head of Forensic Services,
Risk Consulting
KPMG in Qatar

- **Procurement fraud is magnified because of the size and value of projects**
- **Government and company corporate governance fails to keep pace with growth**
- **Fraud and corruption risks intensify in large government projects using intermediaries**
- **Cyber attackers drawn to increasing opportunity and relatively weak defenses**
- **No blueprint for the fraudster, although the senior manager a common face**

Even if fraud is not seen in the media or spoken about, with so much opportunity, you can be sure it is happening. Without fraud defenses, fraudsters are bound to go undetected, siphoning off large amounts of money from both companies and government.

The State of Qatar's economy is booming as it races towards the 2022 FIFA World Cup, with large infrastructure and development projects tempting opportunist and predator alike.

"With an economy growing this fast, corporate governance needs to keep pace or gaps will appear with fraudsters seizing the opportunity."

Government plays a large role in the economy of Qatar, owning or managing most of the significant players especially in the energy sector.

With organizations still struggling to put good corporate governance in place, the government is taking action under an intensifying international spotlight. The recently formed anticorruption watchdog, Administrative Control and Transparency Authority (ACTA), is focused on eliminating practices that hinder transparency. It monitors ministries and agencies to probe allegations of abuse of power or public funds.

Procurement fraud in Qatar tends to be extremely large, mostly because the procurement contracts are highly lucrative. This pay-off tips the scale for the employed opportunist and attracts more organized fraudsters. Procurement processes are particularly vulnerable to subversion by personal relationships or connections, known as "wasta," especially in government contracting.

With poor internal controls and absent fraud deterrence, government and companies have so far failed to put up much resistance to inside opportunists and organized criminals. With integrity vetting of suppliers and subcontractors being a key fraud deterrence measure, the absence of disclosure laws among public officials creates more opportunity for abuse.

While the recent focus on transparency by government may help, how much will be determined by the level of regulation and enforcement.

"KPMG investigations show no real blueprint of a fraudster; we see a different mix committing fraud – locals and expats. Senior management is still in pole position to defraud companies of serious amounts, and currently many of these positions are filled by expats."

In Qatar, generally perceived to have little in the way of petty corruption and bureaucracy having a highly efficient regulatory system, the prime prospect for fraud and corruption continues to attach to larger contracts and the use of intermediaries.

Attracted to the wealth and opportunity, multinational organizations are trying to set up shop, which entails entering into a joint venture with a local business partner. As more development projects are expected, such as Qatar's Doha Metro project, more high-value procurement can be expected.

"Multinational organizations may be exposed to risks if they underestimate the difficulties of rolling out global governance and control practices in a country that is still making its way to a mature corporate governance culture."

With its growing international profile, organizations in Qatar are being increasingly targeted by cyber attackers; recently, malicious attacks on energy companies seriously disrupted business for weeks. With objectives ranging from political agendas to pure greed, the cyber attacker has many faces.

"The right level of information technology (IT) security is a business imperative – deciding what this means is the challenge. With the cyber crime draft law in play, which will make IT security compulsory, Boards and management will need to grapple with this complex area to find the best defense line given cost and benefit."

Although approved, the cyber crime draft law continues to be debated given concerns that it impinges on freedom of expression on the Internet.

Looking forward

"Even if fraud is not seen in the media or spoken about, with so much opportunity, you can be sure it is happening. Without fraud awareness and detection methods, fraudsters are bound to go undetected, siphoning off large amounts of money from both companies and government."

The vigor of the government's enforcement and new ACTA will be key influences on what the fraud landscape looks like over the next five years.

"There are no indications as yet that the profile of the fraudster is about to change radically in the near future; it could be anyone, depending on who has the opportunity on the day. The key to unlocking a company's fraud risk is finding ways to change behavior."

Arindam has over 16 years of consulting and forensic experience. He has conducted several investigations for companies in South Asia and the Middle East, helping them detect fraud and take remedial action, including implementation of integrity and compliance programs. Aided by an Advanced Diploma in Computer Application and a Diploma in Electrical Engineering, Arindam has also assisted clients to take a more proactive approach; he has led a number of fraud risk management engagements, conducting fraud and misconduct diagnostics and working with clients on ethics and fraud awareness.

Russia

Ivan Tyagoun
Head of Forensic
KPMG in Russia and CIS

- **Collaboration with third parties key to fraud in Russia**
- **Smoke and mirrors of silent partners and side agreements means more fraud risk**
- **Russian underground economy democratizes cyber crime**
- **Cyber the new crime scene for fraud, data theft, intellectual property theft**
- **Integrity vetting – the new antivirus for business**

The issues we deal with most often in Russia are procurement fraud and bribery and corruption – any area where there is a nexus between business and government.

Russia is certainly a land of extremes: nine time zones, a top ten world economy, extensive mineral and energy resources yet rated as one of the most corrupt countries in the world.

"The Russian government has sent some strong signals that the attitude to fraud and corruption is changing."

Russia hosted the G20 Leaders Summit in September 2013, shortly after the B20 Summit, where international business formulates recommendations to leaders on, among others, transparency and anticorruption. The B20 meeting led to much local publicity, mostly to raise awareness in Russia on combating corruption.

Ranked 133 of 176 on the 2012 Transparency International Corruption Perceptions Index, Russia languishes with the likes of Iran, Honduras, and Nigeria. It also scores poorly on ease of doing business, prompting international headlines to ask whether Russia is too corrupt for international business.

The last quarter of a century has seen significant change in Russia's socioeconomic-political environment. Practices like silent partners, verbal agreements, trusted contacts, facilitation fees, and intermediaries are part of the Russian paradigm – a society of influence.

But, Russia is moving forward as government extends anticorruption legislation[1] requiring organizations in Russia to implement measures such as ethical codes of conduct and procedures for ethical practices. This follows hot on the heels of Russia joining the OECD[2] Anti-Bribery Convention in 2012.

"In the course of our due diligence work, we do not yet see many bribery and corruption protocols. But, changing behavior and mind-sets takes longer than amending legislation."

[1] Federal Law No. 273-FZ effective January 1, 2013
[2] Organisation for Economic Co-operation and Development

Organizations in Russia are now more aware of issues linked to corruption and both local and international anticorruption legislation, in part a spillover from foreign companies and multinationals reacting to pressure from regulators policing the U.S. Foreign Corrupt Practices Act and the UK Bribery Act.

"While corruption was endemic in Russia, there are signs of a clawback. People are no longer overtly corrupt, as a stigma is beginning to associate with this behavior."

With more focus on corruption, companies prefer not to pay bribes themselves, turning rather to third parties.

"We frequently see agents or third parties like customs agents pay a bribe on behalf of a company, then invoicing for apparently legitimate services to refund this outlay. The invoice to the company looks like a legitimate fee for services so it is difficult to detect."

Employees who are not managers are also involved in bribery and corruption, as they are under constant pressure to increase sales or meet targets to earn bonuses.

Procurement fraud is frequently seen in KPMG investigations, usually involving management setting up contracts with related-party suppliers, suppliers overcharging or not delivering in terms of their contract.

With tightening economies worldwide, contract compliance is taking center stage with edgy interpretations being applied to contracts causing significant losses to companies, although often undetected due to the paucity of controls covering contractual relationships.

The issue of silent partners, and silent or verbal agreements and side agreements, is a dominant theme in Russia, harking back to old habits. Integrity vetting of companies and of vendors in the supply chain is now the equivalent of business antivirus software for local companies and foreign investors.

KPMG investigations show fraud across sectors, although the fraud that tends to follow corruption occurs more frequently in sectors where business overlaps with government institutions like pharmaceuticals and energy.

While not topping the list, employee embezzlement and asset misappropriation are still threats to companies, as is financial statement fraud. Bogus employees, for example, are added to the payroll on management instruction; these employees turn out to be relations or friends of management.

Senior managers and management continue to feature as the typical fraudsters responsible for the most costly frauds. But, in Russia, the inside fraudster is seldom alone, preferring to collaborate with third parties to benefit from the guise of legitimacy.

The level of oversight exercised by Boards has an ongoing question mark worldwide. Most local Russian companies have internal controls and internal audit, but compliance and risk management is less in evidence. Russian companies wanting to attract international investment or play internationally are now realizing the need to invest in governance, risk, and compliance frameworks.

"Fraud prevention is not high on the agenda in Russia, but companies are beginning to come to KPMG for help with fraud prevention."

Russia has a long association with cyber crime, with a thriving underground economy trading in personal data. The Russian underground is said to have

"democratized" cyber crime, headlined by renowned hackers and powerful cyber crime organizations and networks.

"Cyber crime has brought a different fraudster, but it is difficult to say who that is. The problem with this crime is that you cannot easily see the angle of attack."

Despite the crime scene shifting from office to cyberspace, KPMG investigations show motivation has not changed. People under financial pressure remain more likely to turn to fraud, although for management, the opportunity is about the third Mercedes – hard core greed.

"We do not see one profile that commits fraud – all types commit fraud if opportunity presents."

Looking forward

"The trend is that fraud is more likely to be from a cyber attack. We expect things like Trojan software to increase, with companies more exposed to data theft and diversion of assets through increasingly mobile technology."

Bribery and corruption cases are likely to rise with the new focus on antibribery legislation, although general fraud will be close behind as company defenses still offer little resistance.

Despite new initiatives, for many local and international observers, the jury is still out on how corruption will play out in Russia. Its anticorruption legislation has no teeth with few punitive sanctions for noncompliance, so much will depend on how vigorously and impartially government enforces anticorruption initiatives.

Ivan is an experienced Forensic professional with expertise in fraud investigations, anti-bribery compliance reviews, forensic technology, anti-fraud and anti-corruption systems implementation. He joined KPMG's network of firms in August 2012, having previously worked in the forensic departments of other major professional services firms and international corporations. Ivan has successfully managed numerous fraud investigations, disputes, anti-bribery and FCPA compliance reviews for clients in Russia and the CIS in the banking, energy, oil and gas, pharmaceuticals and FMCG industries. Ivan has extensive experience working with cross-border, international and multidisciplinary teams, supporting independent lawyers, internal auditors, compliance officers, and collaborating with colleagues and specialists in all other advisory functions.

Kingdom of Saudi Arabia

Altaf Dossa
Director, Advisory, Head of Forensic Services KPMG Gulf Holdings (Saudi Arabia, Jordan, and Kuwait)

- **Insider fraudsters get more sophisticated, from diverting payments to setting up fake contracts**
- **Companies deal with fraud prevention as fraud dialogue comes to the fore**
- **Cyber attacks still focused on financial sector but on the increase**
- **Fraudsters aided by culture of trust**
- **Companies face increasing threat of data theft**

Fraud, bribery, and corruption are being tackled more openly with these issues now part of an ongoing dialogue. We are receiving more requests from clients to assist them with fraud risk management.

Saudi Arabia, the largest Arab state in Western Asia, has a population of just over 28 million people, with approximately a third being foreign expatriates. While Saudi Arabia has much to distinguish it from other countries, such as having the world's second largest oil reserves and vast natural gas reserves, its fraud landscape bears striking similarities to the rest of the world.

"Many of the cases KPMG investigates involve senior managers that have overridden existing controls or have free reign because of the absence of compliance controls or systems."

The insider or trusted employee is the dominant face of the fraudster in KPMG investigations worldwide, showing that opportunity, including capability, is a key enabler of fraud.

While employee and management fraud continues to dominate, there have been some subtle changes to the fraud landscape.

"Over the last two years, we have seen more complex fraud scenarios perpetrated by individuals. While previously internal fraudsters diverted company funds via fictitious expenses or ghost employees, they are now diverting company contracts to organizations they create with similar names in other jurisdictions."

Saudi Arabia has offered fertile ground for the fraudster in the past. Being a rich country with a large expatriate labor force, it has inherent fraud risks; diverse cultures and mind-sets, and shifting managements, increase the risk of fraud across sectors. However, change is in the wind.

The Saudi government has started to turn the spotlight on the governance of companies and agencies, beginning with implementing requirements for these organizations to have a proper code of business conduct.

Technology also plays a large part in changing the fraud dynamic in Saudi Arabia, as the cyber criminal features more prominently in attacks on company assets.

"Fraudsters in the region are more acquainted with using technology to perpetrate acts of fraud, yet legislation and the judicial system have not adjusted for the new crime scene – cyberspace. For example, the courts are not yet familiar with the types of evidence presented in cases of cyber crime."

Saudi Arabia mirrors global trends; cyber crime is increasing although still largely concentrated on the financial sector with attacks ranging from ATM attacks to online banking fraud. The Central Bank, the Saudi Arabian Monetary Agency, is responding to this increased risk by emphasizing cyber crime in its regulatory circulars to the financial services institutions.

"We cannot compile a profile of the cyber attacker as this person is cloaked by the invisibility of cyberspace. So far, we've seen the 'hacktivist' with a political agenda opposing adoption of Western culture and threatening key institutions with denial-of-service attacks, and the cyber fraudster out for financial benefit using middleman tactics or social engineering to obtain access credentials to bank accounts."

The culture of trust in the Middle East also assists the fraudster, as citizens and business people alike still pride themselves on the level of trust in business.

"We often see fraudsters able to carry out their acts of deception by abusing this culture of trust. Social engineering is becoming a serious threat to companies and individuals worldwide."

Social engineering, or "human hacking" as it is called, is the practice of using social engineering techniques to deceive someone, in person, over the phone or in cyberspace with the intention of breaching security and perpetrating a crime – con games – and they include the old scheme whereby the creditor's clerk is convinced of a change in the supplier's bank account details.

"We don't think the complexity of the fraud acts we are seeing will increase dramatically for the simple reason that companies are not closing all the gaps, so fraudsters will continue to use these old opportunities."

Most organizations appear to be taking a mechanical approach to managing their risk and establishing a control environment. Managements tend to rely on GRC (governance, risk, and compliance) software to check the box that they have controls in place to prevent and detect fraud. Much of effective fraud deterrence, however, relies on management analyzing trends in the broader environment, and dealing with the human element inside and outside of the organization.

"Managements rely on internal audit functions to identify the risk of internal fraud and misconduct. However, very often internal auditors have little prior investigation or forensic experience, making it difficult to develop the mind-set required to properly interpret the information and the fraud risks."

Looking forward

"The future fraudster will need to be 'tech savvy,' meaning cyber criminals, as technology continues to dominate business processes and present the greatest prospect for illicit gains."

However, although technology will continue to become more of an enabler of fraud, the profile of the typical fraudster is not expected to change in the medium term.

"We also see the theft of data or leakage of confidential information as a growing threat for organizations in the Kingdom. With digital technology and black markets, an organization's information is even more vulnerable to inside employees and external hackers."

Globally, many companies have not yet responded to the increased threat of data theft or leakage of confidential information. Solutions do not only require sophisticated technology, but also basic fraud and ethics training for the human element in the organization.

Altaf has over 16 years of experience, 10 of which have been in crime compliance reviews and information security working at KPMG Luxembourg and in the UK. Prior to joining KPMG in Luxembourg, he worked for USAID in Washington, DC, UNDP in various African countries, and the Francophone organization based in Mauritius.

With KPMG, Altaf has worked in many European countries, covering fraud risk management, regulatory compliance including U.S. FCPA and SAMA requirements, financial misconduct investigations, and bribery and corruption investigations. Altaf helps clients design and implement appropriate fraud detection technology and works with clients conducting information security audits.

Singapore

Lem Chin Kok
Partner,
Forensic Services,
KPMG in Singapore

- **Employee fraud in Singapore perceived as the largest fraud threat**
- **Most companies believe that external statutory audits detect financial statement fraud**
- **While business and technology changes, companies rely on defenses from 10 years past**
- **Local companies vulnerable in the region to procurement fraud as they fail to see the signs**
- **Corruption back on agenda as local companies unaware of employees' practices in the region**

The culture in Singapore tends to procure at the lowest price. Many companies do not appreciate the warning signs behind goods or services being sold or rendered at half price. Missing the signs can mean quality issues, nondelivery, and even not knowing how you have been defrauded.

One of the four Asian tigers, Singapore, is home to numerous local and multinational businesses; it serves as a hub for trade in the region with countries like Malaysia, Hong Kong, China, Indonesia, and Australia.

With sophisticated and transparent financial markets, strong regulation, and relatively little corruption, Singapore has become a major international banking, shipbuilding, and petroleum center with a busy seaport.

This thriving economy, insulated from the global crisis, provides plentiful opportunities for the fraudster. KPMG's 2011 fraud[1] survey indicated that while the number of companies falling victim to fraud in Singapore had not increased significantly since 2008, one in four companies were being hit harder and more frequently.

Employee fraud in Singapore is perceived to be the largest fraud threat facing companies. However, no one profile fits all fraudsters.

> **"We do not see an obvious profile for the fraudster; our experience shows that most people can commit fraud if confronted with the right trigger."**

In Singapore, like other countries, the fraudster most frequently seen in KPMG investigations remains the opportunist – the person whose circumstances precipitate action.

Worryingly, many companies in Singapore have few fraud deterrence measures in place, making them vulnerable to internal fraudsters and even external perpetrators. KPMG surveys in the last two years revealed less than 40 percent of companies using fraud risk management and conducting fraud risk assessments. Interestingly, the majority believed that external statutory audits were sufficient to detect financial statement fraud.

> **"Cyber crime has increased and we expect cyber attacks and high-tech fraud to grow exponentially. Even in the face of rapid changes in the business world, some companies in Singapore have not changed their internal controls and defenses in 10 years. What was effective 10 years ago is no longer effective."**

1 KPMG Singapore Fraud Survey Report 2011

With advancing technology, protecting proprietary information is an increasing challenge for businesses and individuals alike; organizations still have gaps in their IT security and fraud defenses partly due to the difficulty of developing a real understanding of how high-tech crime is perpetrated and how to prevent it.

Singapore is rated in the top five least corrupt countries in the world by Transparency International's Corruption Perception Index.

"In Singapore, relatively speaking, there is very little corruption, mainly because the enforcement is stringent, and business is conducted in a transparent way."

Singapore has a long-standing anticorruption agency, the Corrupt Practices Investigation Bureau (CPIB), and related anticorruption legislation gives the CPIB extensive investigative powers.

One risk for local companies is the widespread lack of awareness of local and international anticorruption legislation. Companies are slow to respond to warning signs.

Seventy-nine percent of the companies in Singapore surveyed by KPMG[2] in the last two years said they were unaware of how their organization dealt with bribery and corruption risks in the regional economies, with half describing a flexible approach, offering payments and gifts when culturally necessary.

"While companies seldom engage in corrupt practices in Singapore, in some cases, those same companies pay bribes when they do business in the region."

A common thread across the globe is the crucial role of active enforcement in deterring bribery and corruption, and other financial crime. More regulated industries investigate these issues more readily than companies in less regulated industries where the decision to investigate rests with management. In Singapore, companies are generally disinclined to prosecute fraudsters, preferring to terminate employment. However, things may be changing, as recent indications suggest companies in Singapore are becoming more willing to pursue the fraudster.

While fraud takes many forms in Singapore and is seen in all industries, local companies are especially vulnerable to procurement fraud when doing business in the region, missing many of the warning signs and experiencing more fraud by procurement staff and management than multinationals. There is a tendency for companies in Singapore to procure goods and services based on price, frequently missing the key warning sign – the unreasonably attractive price – which can mean quality issues, nondelivery, and fraud.

For multinationals, the major concern is bribery and corruption, and the U.S. Foreign Corrupt Practices Act. Multinationals in the region are less likely to be cheated by procurement-related fraud having stronger procurement processes in place, and placing more emphasis on the qualitative aspects of bids.

Procurement abuse is exacerbated by frequent conflict of interest, with people in the region belonging to extended families, and companies not yet updating their controls and risk management to cater for third parties such as contractors.

"The way we do business has changed – we no longer do everything ourselves so controls need to change. Few companies carry out integrity checks or vet their supply chain partners."

2 KPMG Singapore Fraud Survey Report 2011

Looking forward

The way we do business is going to change even further and faster than in the last two decades. The electronic world poses significant challenges for business, challenges for which many businesses are not wholly prepared.

> **"If you don't see the changes in the environment and in tandem change how you operate, there will always be gaps, and the company will always be exposed. Regulation forces some industries to respond to certain risks, and this means these companies will be less vulnerable than others."**

Collusion means any control environment has inherent limitations. Fraud risk management is better placed to effectively deter fraud because it goes beyond the controls and addresses fraud risk holistically. The challenge for managers is calibrating controls and antifrauds correctly, striking the balance between cost and defense.

Even as cyber crime increases, the employee with knowledge and opportunity is expected to continue to be the dominant fraud threat for companies in the immediate future.

Lem has extensive experience in white-collar investigations in the region, spending 11 years with KPMG, and 5 years with the Singapore Police Force, including the Commercial Crime Squad. Lem, as a qualified chartered account and former regional finance manager of a Singapore listed company, has an in-depth understanding of the challenges facing businesses in Singapore, and frequently assists companies with their fraud awareness and fraud defenses.

South Africa

Déan Friedman
South African &
EMA Investigations Leader

- **A morphing fraudster as changing environments demand new capabilities**
- **Capabilities of the fraudster change in pace with an evolving environment**
- **Cyber environment expected to dominate financial crime in future**
- **Cyber criminal, invisible but aggressive, exploiting victim safeguards to steal assets**
- **Investigators must come to terms with new behaviors to spot the fraudster**

In EMA, and globally, the cyber criminal has introduced a very different behavior that investigators are still coming to terms with; this criminal's behavioral aspects provide some of the tangibles we can use to help identify what happened and who perpetrated the crime.

"While profiling criminals is a contentious probative activity, looking at the behavior implicit in the commission of the crime as well as how this changes over time can help identify the crime and the perpetrator."

While changing environments, such as new technology or socioeconomic factors, bring with them new opportunities for fraudsters, they also give birth to new fraudsters with new capabilities and changing behaviors.

As the pace of change in our world increases, organizations should seek to understand the ever-changing behavior of the fraudster if they are to mitigate the risk of fraud and then respond quickly to such crimes.

"Investigating crime means understanding the behavior implicit in the commission of the crime, and how this changes."

The behavioral profile of the fraudster is informed by the consistency in where the crime takes place, how it is committed, and what means are applied to commit the crime.

Many years back, syndicates would steal a checkbook, forge the drawer's signature, and present the check at a bank for payment using a false identity document. For good measure, they would tap into the bank's telephone line as it phoned the client to authenticate the check. We became used to investigating this behavior (and perhaps have somewhat forgotten how to do this in the modern world where checks are no longer used), driven by more psychological and real profile measures relevant to the time, that is, a criminal gang that needs money finds itself in a certain socioeconomic environment with certain skills.

Then, in Europe and other countries with sophisticated bank systems at the advent of the Internet, checks were no longer used; forging negotiable documents was replaced by forging or making fraudulent transactional documents – the new behavior of the day.

Again, we became used to investigating this behavior albeit with a slightly different approach. These "new" crimes, however, were driven by the same psychological and real profile measures found previously, except that good forging skills were no longer required. The environment had evolved, requiring new capabilities and behavior from fraudsters.

It is this fast-changing technology environment that has engendered a new type of fraudster – the cyber criminal.

The cyber criminal strikes at the heart of protection measures organizations and people had put in place, which previously needed deception and guile to overcome. The cyber criminal uses those same protection methods to commit the crime, yet cloaked by the environment of computer, cloud, Internet, and so forth.

While the traditional means used by typical fraudsters from a few years ago convinced victims to impoverish themselves or to sacrifice a principle, the cyber criminal's behavior is more aggressive. It takes direct control of the assets by which the victim is impoverished and, perhaps more importantly, assumes direct control of the very governance set in place to safeguard those assets. This appears to be a significant change in the profile of a fraudster.

The behavioral change aside, these crimes are still driven by the same psychological and real profile measures as found previously. But, the behavioral aspect of the cyber criminal is what implies there will be a somewhat different way of investigating many of the financial crimes of the future.

So, from the forger's pen to the code writer, from hiding behind a disguise to hiding behind the Internet, cloud, and the like, the capabilities of the fraudster have shifted in step with the evolving environment. It is this concept of capability – the traits and skills of the fraudster – that is the morphing factor driving the behavior of the fraudster and ultimately the profile of the fraudster.

In the 2007 KPMG survey of the profile of a fraudster, albeit confined to Europe, the Middle East, and Africa, KPMG found that in 69 percent of its investigations, the fraudster was someone employed by the victim – the internal fraudster. By 2011, the comparable result was 90 percent with KPMG seeing increasing numbers of frauds committed by insiders.

"As our world migrates to a full electronic universe and integration, these statistics may reverse dramatically, with the added complication of invisibility of the fraudster."

Looking forward

As the cyber environment is expected to be the dominant medium in the financial crime of the future, organizations and investigators are under pressure to get to grips with this new behavior if they are to spot this fraudster – the cyber attacker – and head him or her off at the pass.

"To unravel the frauds of the future, the best investigators will be those that are able to reduce large amounts of data to identifiable events with good technology solutions, operating seamlessly across borders and with good corporate intelligence capability to give them quick historical and geographical reach."

Déan Friedman leads KPMG's Investigations Network in the Europe, Middle East, and Africa region. He is the partner responsible for investigations and corporate intelligence in KPMG's South African firm and also renders asset preservation services. His experience crosses several industries and geographies. He formerly prosecuted fraud and other commercial crime cases on behalf of the state in South Africa's regional and high courts.

South Korea

Hee Jun (Harry) Kim
Partner, Head of Investigations
KPMG in Korea

- **Bribery of government officials continues to overshadow business in South Korea**
- **Lagging systems make family-owned conglomerates vulnerable as top managers turn fraudster**
- **A tougher approach to enforcement of white-collar crime appears on the horizon**
- **Companies look to strengthen information technology (IT) defenses as hackers steal customer information**

There are two dominant fraud themes in South Korea – bribery of government officials and fraud committed by the top management of organizations.

South Korea, one of the Asian Tigers, is situated in East Asia. It has just over an estimated 50 million residents with land or sea borders with North Korea, China, and Japan. Since its bankruptcy in the Asian economic crisis in 1997, South Korea's economy has recovered in leaps and bounds, joining the ranks of Japan, the United States, France, and the United Kingdom to name a few as a member of the 20–50 club in 2012 – a club of countries whose population surpasses 50 million and per capita income reaches US$20,000.

South Korea is ranked 45 out of 176 countries on Transparency International's Perception of Corruption Index 2012. Despite improving its position on the index from the previous year, bribery of government officials is still a frequent occurrence, especially by suppliers in the public procurement process. Recent allegations of bribery and corruption in the energy sector show that this practice continues to overshadow business in South Korea.

Fraud by a company's top management, such as embezzlement and asset misappropriation, is a dominant feature of South Korea's fraud landscape.

Unusually, South Korea has many high-profile family-owned conglomerates, a number of which have experienced large frauds in recent times. These conglomerates, locally known as "chaebols," are typically multinationals controlled by a chairperson with power over all operations.

Chaebols have dominated the economy for some time and continue to do so despite new regulations after the Asian economic crisis aimed at curbing their overriding influence in the market. These new regulations include antitrust laws, inheritance taxes, and strengthened accounting regulations.

Having started out as family businesses, many family-controlled corporate groups have experienced exceptional growth. In many cases, however, the internal systems and processes of these conglomerates have not yet caught up with the governance, risk, and compliance structures necessary for large corporations. This creates inherent fraud risk, which provides ample opportunity for fraud and corruption.

Corporate frauds perpetrated by the top management of chaebols is said to have a significant impact on society by, among other things, causing business delays and potentially canceled investment due to a lack of leadership.

South Korea's courts have just sentenced leading business executives from the Hanwha Group and the SK Group to jail time and a fine for misappropriating company funds. While these sentences are seen as part of government's tough new approach to high-profile corporate frauds, its resolve is still to be tested as these sentences go on appeal. In past times, chaebol chiefs escaped with suspended sentences for white-collar crime convictions.

While there is no specific factor that drives the occurrence or type of fraud in the country, the absence of internal controls and fraud deterrence measures in companies allows more fraud to take place.

"The owner of Samsung recently emphasized the need for companies to set up internal controls to minimize fraud, which is prevalent in companies across the Samsung group."

Companies in South Korea, like elsewhere, have increasingly implemented IT systems; business now relies heavily on electronic and automated systems. This is especially the case in many of the country's main industries: electronics, telecommunications, automobile production, chemicals, and shipbuilding.

"Because of the extent to which businesses now rely on IT systems, it is difficult for any fraudster to commit fraud without accessing these systems and manipulating the data. Fraud prevention and investigations increasingly rely on forensic IT technology to detect fraud through data mining."

Cybercrime has also become a more common theme, with cyber attacks being used to obtain personal information in a preface to fraud or other illicit activities.

"We have seen cyber attacks more frequently, where hackers attack industries like the financial sector and the Internet industry to obtain personal information. For example, Internet companies have been hacked by professional hackers for customer information that was later sold on the black market for use in illegal activities."

Because of the increasing risk of cyber attacks and the vulnerability of personal information, regulations have recently changed, now requiring South Korean companies to enhance the security of their IT systems.

Looking forward

There is little doubt that a slowing economy places pressure on the middle class. Increasing wealth disparity in society brings the additional risk of fraud committed by people, especially employees, trying to hold on to a lifestyle.

"While simple white-collar crime such as investment fraud and simple acts of embezzlement are expected to continue to occur, we also expect the more complicated fraud schemes to appear more frequently."

However, the government's continued efforts to combat fraud and corruption may be the counterweight that will reduce this crime in the future. The government's initiatives to prevent misconduct by government officials, and the push to apply regulations without exception, extending to chaebols, may build further momentum in the drive for transparency and the pursuit of fraudsters in South Korea.

Harry has led some of the most complex and challenging Forensic engagements in Korea for local and global clients. He has substantial experience in investigative and integrity engagements with regards to the FCPA. Harry joined KPMG's network of firms in 2001 and has worked in the field of forensic accounting and investigation services since 2004.

He has performed FCPA reviews on internal processes and procedures of global pharmaceutical and healthcare companies and identified any non-compliance issues on their internal policies. In addition, he performed several investigations and reviews on US companies to identify any non-compliance issues particularly FCPA related.

Spain

Angel Requena
Partner,
Head of Fraud Prevention and Detection
KPMG in Spain

- **Fraud on the rise cutting across industries with companies putting up a weak defense**
- **Government is a prime target for internal fraudsters and third parties**
- **Unaware of new fraud risks and legislation, Spanish companies doing business in foreign countries face losses, huge fines, and criminal sanction**
- **Cyber attacks threaten companies; companies still suffer most damage from insiders**

The economic situation in Spain is not good, and in this climate, organizations refocus priorities; to reduce fraud, they need to consider implementing updated systems, standards, and technology.

"Mostly, KPMG investigations encounter fraudsters as people with relevant decision-making powers and the opportunity to commit the fraud – senior management and directors."

KPMG investigations show that senior executives continue to exploit opportunities to defraud employers of very large amounts. Fraud in Spain, however, is no respecter of industry or status.

Government is a prime target for the internal fraudster and third parties, who take advantage of lagging internal controls and limited fraud deterrence. Attracted by opportunities in the supply chain and other areas with quick access to cash like grants or social security, fraudsters threaten all levels of government in hard economic times.

Smaller local savings banks in Spain ("caja") also face significant issues with widespread bankruptcy and investigations into dubious and sometimes political investment decisions by managing regional governments. Some banks are also subject to reporting fraud as they face allegations of delayed registration of bad loans to avoid declaring losses.

Lack of fraud deterrence and internal controls is not just a question of economics; it is also a question of culture. Not peculiar to government, most companies in Spain have inadequate fraud defenses – with the possible exception of the financial sector, which has had to upgrade defenses by dint of regulation. But, some organizations are starting to take action.

"KPMG in Spain is currently working with a government department to implement fraud measures and techniques to trigger early warning signs of fraud or other irregularities."

Following enormous growth, the construction and real estate sectors have hit hard times; significant cost cutting in the last three to four years has left many companies looking further afield for work, for example, in Latin America. However, more frauds in these industries may come to light as extensive investment in infrastructure provided ample opportunity for fraud, especially in procurement as the need for licenses and permits tempted kick-backs. Third-party fraud is often a focus in KPMG investigations, with companies

falling short on integrity vetting of suppliers and business partners.

Fraud in the financial sector in Spain is not always the typical fraud seen elsewhere, but rather the result of questionable investment decisions relating to political investments coming under scrutiny, which can contribute to losses of banks and their clients.

KPMG's investigations frequently involve technology, with fraudsters using sophisticated technology especially in the banking, insurance, and telecommunication sectors.

"In one case, employees manipulated the company's digital communications to simulate both decision and authorization for automatic payments. Very large amounts were taken from the company's bank account and paid into a foreign bank account, making them impossible to recover – this is where fraud is moving to."

In the past, fraud was concentrated in the larger sectors like government, financial, construction, infrastructure, and real estate. Now the pressure on management and Boards to produce good financial results and meet shareholders' expectations has seen more sectors affected by fraud.

"Our investigations include financial statement frauds involving large listed companies, where financial statements are manipulated to meet certain growth expectations. Reporting fraud is certainly not limited to any one sector."

Spanish companies have to navigate fraud pit-holes in foreign jurisdictions as well as at home. Spanish investment in Latin America has intensified with companies doing more of their business abroad. Predictions are that by 2015, some Spanish companies' operations in Latin America will generate more revenue than the local market.

"Spanish companies should carefully consider possible legislative and fraud risks when entering new markets. Being unaware of how different cultures and business practices affect a company's operations, code of conduct, and legislative responsibilities can be lethal."

To mitigate the fraud risk of operating in a foreign country, companies should ensure staff in remote offices receive strong ethical guidance from the company's code of conduct and fraud awareness training.

Spanish companies with operations connected to the Unites States and United Kingdom in particular will need to be aware of the long arm of U.S. and UK anticorruption legislation – that is very actively enforced.

Looking forward

As legislative risk in Spain increases in areas like tax fraud and bribery and corruption, managements may be reprioritizing internal controls and fraud risk defenses. More rigorous international enforcement is expected, requiring companies to be increasingly vigilant regarding global compliance.

Technology will continue to influence who can access a company's assets. Despite tough times, information technology (IT) security and fraud testing have become nonnegotiable for most organizations, especially those doing business in high-risk jurisdictions.

"While cyber attacks introduce the threat of the external fraudster, we continue to see the internal fraudster causing the most damage to organizations in Spain. It seems the perpetrator with the most opportunity to defraud will continue to be a dominant fraud risk – currently, this appears to be the senior manager."

The current economic climate has seen Boards and management prioritizing controls and fraud risk management a distant second, which has left organizations more exposed than ever.

However, simple fraud deterrence such as fraud awareness training and supplier vetting seems relatively cheap compared to the cost of fraud.

Angel, a registered auditor and forensic specialist, has 25 years' experience working on fraud prevention and detection projects in diverse sectors. He has led a variety of fraud investigations, some involving the analysis of digital evidence, including domestic and international investigations into allegations of bribery and corruption in the industrial sector, government investigations involving digital evidence recovery, and banking fraud. With postgraduate studies in technologies and fraud, Angel assists clients to implement sophisticated systems for fraud prevention, continuous monitoring, and fraud prediction tools.

Sweden

Martin Krüger
Partner in Charge, Forensic
KPMG in Sweden

- **A culture of trust is a key catalyst for fraud**
- **Organizations in Sweden behind on the compliance and control curve**
- **Public sector procurement is a gift for the fraudster**
- **Deterring fraud requires a back to basics approach**

Frauds frequently occur because of a failure to have a basic control in place. Our investigations show, for example, that management does not always check supporting documentation before authorizing a transaction. This goes back to Sweden's culture of trust.

Sweden's culture of trust is a key catalyst for fraud in the country.

> **"The perception of little fraud in Sweden is common, driven largely by Sweden's culture of trust, which assumes people are moral and will behave according to established mores."**

It is thus unsurprising that historically, Swedish companies and public sector organizations have weak internal control environments and continue to lag the compliance and control curve. Much of business's attitude has been honed in a culture of values over regulation.

> **"In a number of organizations, we have come across a culture of not seen, not heard, not guilty. Top management frequently choose not to invest in internal controls and fraud deterrence seeing it both as a statement of mistrust in its people and as unnecessary since fraud happens to others."**

This attitude also serves organizations poorly when talking about fraud, fraud awareness, and fraud risk management, all of which require a skeptical mind-set and ongoing dialogue.

KPMG investigations show that companies that fall victim to fraud have no fraud risk strategy or fraud risk management system in place, only getting to grips with their fraud risks once exposed to loss or bad publicity.

Swedish organizations rely on light armor in the face of increasingly costly attacks by the internal fraudsters, the external contractor, and even the cyber attacker. However, signs of change are afoot.

> **"We are seeing dialogue on transparency, risk, and fraud as Boards become more aware of financial, legislative, and reputational risks. They are focusing more on compliance and risk each year, leading to requests for fraud awareness training and whistle-blowing lines."**

Companies worldwide are aligning their responsibilities for governance, compliance, and risk management, using integrated GRC systems to use synergies and avoid gaps.

The internal fraudster thrives in Sweden's low compliance environment and

benefits from the lack of sanction and consequences once detected, with fraudsters being recycled into the business world, unmarked and untracked.

Fraudsters most often find gaps and opportunities to defraud the public sector, particularly in the supply chain.

"Conflict of interest in public procurement is rife resulting in government paying more for services, or paying for services or goods not provided or even paying for private costs of public officials."

More robust government and public sector internal controls are needed to combat this level of abuse. Some sectors have recently been especially exposed to issues in the supply chain, including building and construction and industrial cleaning.

"With little staff or supplier rotation in the supply chain, we see the same officials using the same suppliers for prolonged periods allowing misconduct to roll on. While larger companies use business intelligence to vet suppliers, it is not extensively used in government."

While public sector procurement fraud has seemed close to endemic at times, there is now growing public interest in curbing this type of abuse. Despite being ranked the fourth least corrupt country in the world by Transparency International, corruption in Sweden is now firmly on the radar, with revised antibribery legislation coming into force in July 2012. A number of recent high-profile bribery cases (the bribery allegations against TeliaSonera AB, the country's biggest phone company as one example) has encouraged organizations and government bodies, including the State Auditor, to rethink the paradigm that corruption in Sweden is not an issue.

"While not as strict as the U.S. Foreign Corrupt Practices Act or the UK Bribery Act, this legislation has received a lot of attention in Sweden. With provisions on negligent financing of bribery, the act creates more legislative risk for organizations and increases the need for effective compliance systems and internal controls."

KPMG investigations reveal that fraud in information technology (IT) departments is widespread but not as might be expected. It is not high-tech fraud, but rather plain misappropriation of company assets stemming from a basic failure in authorization controls – as simple as employees ordering extra laptops or other equipment and taking them home.

While sophisticated IT fraud and cyber attacks do occur, companies are still pursuing external investigations of insider attacks, commonly in collusion with third parties, where opportunists have worked control gaps. Thus, an enforced code of conduct setting the tone from the top and linked to employee employment conditions is key in a fraud deterrence strategy.

"One of our difficulties when clients appoint us to investigate any alleged wrongdoing is they often have no code of conduct or rules, making it difficult to prove misconduct and discharge the employee without criminal proceedings."

Looking forward

As Sweden moves towards a cashless economy, technological opportunity will see organizations more exposed to the cyber attacker, although for now, fraudsters are still using traditional fraud opportunities, and eliminating opportunity requires companies to focus on the basics first.

Although Sweden seems largely unscathed by the credit crunch, certain sectors are under pressure to deliver results, which may translate into more financial statement fraud in the future.

To manage risk, organizations must look outward, scanning the environment for the next threat. With human capital a valuable asset and potential risk, human resources (HR) departments are considering the impact of "Next Gen" studies on their organizations. These insights may well inform if and how a company's fraud risk changes and what a new fraudster may look like.

Unique case

Sweden has seen a number of recent bankruptcy scandals, with one such case involving a security management company that transported cash for banks and went bankrupt in 2012. A number of client banks reported missing cash which, as it turned out, had been misappropriated and used to finance the company's operations or line the private pockets of its owners. This prompted a call for legislation in the banking sector in Sweden to extend to all organizations in the cash chain – a trend also reflected by the legislation developing with respect to payment services in this sector.

Martin Krüger heads KPMG's Forensic services in Sweden. Martin is an authorized public accountant, with wide experience of forensic investigations and transaction-related work. Specializing in dispute advisory services, he has acted as expert witness in several disputes. From 2008 to 2010, Martin was a member of the Forensic Council established by the Swedish National Economic Crimes Bureau.

Switzerland

Philippe Fleury
Head of Forensic
KPMG in Switzerland

Cindy Loots
Head of Investigations
KPMG in Switzerland

- **Employees turn fraudster overriding controls thinking that this is in the interest of their company, and in some cases in search of good life**
- **Fraudster evasion of standard controls calls for more creative antifraud thinking**
- **Organizations unprepared for escalating threat to intellectual property and information**
- **Swiss companies with foreign operations not seeing the full picture in local color**

Typically, a person commits fraud to fund an extravagant or at least very comfortable lifestyle; we seldom see people turn fraudster to make ends meet. Already well off, we often wonder why they take the risk.

Switzerland, with 8 million German, French, Italian, and Romansh people, is a diverse country with one of the highest per capita wealth levels worldwide. KPMG investigations show that in a lot of cases, employees do not understand the compliance risks that arise for the company when they pay bribes; these employees think that they are acting in the interest of their company. In other cases, a person's financial situation is a key driver of management and employee fraud, but it is less about survival and more about greed and pursuit of *la dolce vita*.

Fraud affects all organizations in Switzerland, from very big companies to very small touching all sectors, and seems to be accelerating as people feel the pressure of the recession.

The fraudster most frequently seen by KPMG, in Switzerland and globally, is the insider, respected and trusted, turned fraudster after years of service.

"The fraudster we encounter is usually the trusted manager or employee in finance; when revealed, most people are surprised, finding the behavior totally out of character."

Switzerland operates via a culture of trust; its corporate culture is permeated by a sense of community and family, making insider frauds particularly damaging for companies.

"We usually find the fraudster overriding controls. While most companies in Switzerland have standard internal controls, a person can root out opportunities after four or five years."

Employees often know a system's weaknesses, or are aware of opportunities for some time before acting on them.

"Something triggers a person to act on information they have had for some time. Missed promotions, poor pay, no bonuses, or unresolved issues at work are often triggers."

Control frameworks can never be invulnerable, especially when faced with a person who intentionally evades the controls and frequently has the position and formal authority to do it.

"Typically, companies do not invest time thinking like a fraudster, just to see what frauds could be committed and how and where their biggest fraud risks are."

Appropriate antifraud measures are more effective than standard hard controls, although best practice points to defense on many levels. Decision makers in Switzerland, as elsewhere, are reluctant to invest in fraud defenses for something they believe will not happen to them.

KPMG investigations show that organizations are most frequently affected by insider frauds involving embezzlement. These include fictitious invoices triggering money transfers to personal accounts, senior executives siphoning off company assets or clients to their parallel businesses, together with increasing financial statement fraud.

"Intellectual property theft is also more prevalent with most data electronically available and easy access to information; we see more cases in this area."

With the well-publicized data security issues in the Swiss banking sector, awareness of data loss, data protection, and data privacy issues is growing, although KPMG investigations show organizations have few controls over intellectual property stored on networks, allowing most employees unrestricted access.

Another emerging trend is the increased frequency of family offices in Switzerland being attacked by inside employees and trusted investment advisors. These offices, set up by wealthy families to manage their investments, operate with few controls and much trust.

Bribery and corruption has received plenty of recent press in Switzerland, with government strengthening its antibribery legislation.

"Many bribery and corruption investigations we conduct for companies in Switzerland are mainly driven by EU, UK, and U.S. regulatory scrutiny."

Enforcement has also tightened locally, however, spurred by aggressive prosecution by Switzerland's courts and authorities. Globally, Switzerland is perceived to have a clean business environment with little corruption, rating in the top 10 least corrupt countries in Transparency International's Corruption Perceptions Index 2012.

"A lot of our work in antibribery and corruption is for local holding companies with issues in their foreign operations, particularly in the more risky jurisdictions."

Holding companies often fail to detect issues like bribery and corruption at local operations as senior executives or head office compliance teams flown in to oversee local operations are not conversant in local conditions or customs.

Although internal employees may dominate embezzlement investigations, KPMG frequently sees third parties involved in bribery and corruption investigations.

"This is a new area for companies, and typically, companies do not screen or vet third parties or agents unless subject to an investigation by, for example, the United States Department of Justice."

With advancing technology, it is easier to commit fraud. In the past, you had to forge a signature; now it is about stealing identities and information, or hacking information technology (IT) systems.

"Banks in Switzerland have sophisticated defenses to expose high-tech frauds, while the defenses in many corporates generally remain pretty rudimentary."

While cybercrime is a threat to companies, particularly in the banking sector, KPMG investigations show fraud in the banking sector can also be very simple; naive employees, unaware of the issues and untrained, provide personal data to outside parties responding to e-mails or telephone calls.

Looking forward

"We expect more frauds to be committed by younger people using sophisticated technology, if not in the next 3 to 5 years, then definitely in the next 5 to 10 years."

Globally, cyber attackers are perceived as a younger generation, situated outside the organization. As with all fraudsters, however, no one face stands out as both organized criminals and insiders appear in cyber attacks.

"There are many possibilities open to a hacker, and based on how open company systems are, we expect to see more crime in this area."

The financial pressure in Switzerland is not expected to go away, and nor is its appeal to fraudsters.

Philippe joined KPMG's network of firms in 2007. He is a Partner and Head of Forensic and is responsible for the Anti-Money Laundering Forensic service line in Switzerland. He also leads the KPMG Advisory practice.

Philippe was educated as an attorney-at-law and from 2002 to 2007 he worked as head of section and management of the Swiss Money Laundering Control Authority in Berne.

Currently Philippe provides services in fraud prevention, detection and response. He specializes in the financial services and markets, and in Anti-Money Laundering matters in Switzerland and internationally.

Cindy is a qualified South African Chartered Accountant, with 10 years Forensic experience. Cindy has experience in the areas of fraud prevention, detection and response, specializing in fraud and misconduct investigations, including anti-bribery and corruption. Cindy has been involved in and led various investigations in Switzerland and South Africa.

Cindy joined the Swiss Forensic practice in 2008 and is currently head of the investigations team, leading and conducting investigations regarding fraud, corruption and bribery as well as assisting clients to improve their systems and processes to prevent future incidents.

Taiwan

Rex Chu
Director, Forensic
KPMG in Taiwan

- **Internal fraudsters at play colluding with outsiders to evade controls**
- **Company internal audits provide false sense of security often carried out in name only**
- **Fraudsters hold all of the cards until companies shine a light on fraud and wayward employees**
- **Lagging controls over information technology (IT) information systems place companies at risk**

Taiwanese companies tend to explain frauds as being 'unintentional' and happening 'from time to time.' In this way, companies protect internal fraudsters and perpetuate the behavior.

Two different types of fraud predominate in Taiwan. The first is dominant shareholders or people in authority embezzling or stealing company assets, with the main victims being other company shareholders or investors. The second is fraud perpetrated on companies by their employees, mostly in collaboration with external clients or vendors; inside fraudsters usually embezzle company assets or engage in bribery and corrupt practices.

Companies in Taiwan believe that they are well prepared to combat fraud having implemented internal control mechanisms and carried out periodic internal audits. However, KPMG investigations show that when fraud occurs, a company's internal audit procedures are frequently unsuccessful in tripping up the fraudster; despite well-designed and functioning controls, internal control frameworks lack sufficient substance and integration with the company's fraud risks to effectively prevent and detect fraud.

Furthermore, because of Taiwan's culture of "not washing one's dirty linen in public," companies often prefer to manage the fraud themselves, communicating privately with their management. Unfortunately, this approach does not deter employees from committing fraud or misconduct, and often results in other employees receiving the wrong message regarding the company culture and its tolerance of fraud. By protecting internal fraudsters, companies often have to deal with significant losses, built up over a number of years, after the fraudster has left and disappeared.

"We have seen that dealing with fraud privately increases both the frequency and the amount of the company's losses. We found that companies who fail to deal with the issue often lose over 1 million dollars even after a fraud is exposed."

KPMG investigations show that fraudsters frequently shift funds between debtor accounts to cover up gaps caused by embezzling debtor receipts. This is called lapping, a scheme to conceal fraud by rolling it over or circulating it between different debtor accounts.

Strong internal audit departments, with a good understanding of fraud and the

company's fraud risks, are usually able to detect red flags which point to practices like lapping and other frauds. By dealing with red flags immediately, management is able to significantly reduce the damage to the company. Prevention, however, is preferable to deterrence after the fact.

Organizations currently rely on information systems to help them perform core operations. Because of this, operational data has mostly become electronic.

"Our investigations show that fraudsters are either given inappropriate system privileges by the company, or circumvent the IT system controls to modify or manipulate information, such as the latest trade, or even embezzle funds or assets from the company."

KPMG investigations show that fraudsters are able to carry out unauthorized actions in a company's information system because of a simple oversight; inappropriate privileges or access rights are often granted to users when their accounts are created on the company's system.

Moreover, tracking global trends, management has a tendency to see IT systems as a control in themselves, assuming information generated by sophisticated systems to be correct. This mind-set does not only stem from the sheer volume of data and large number of daily trades, but generally, managers also do not consider that employees would modify or alter the inputted data.

"Many companies fail to develop adequate detection or warning reports to provide alerts on unusual transactions in the system, so it is difficult to detect and track unusual activities."

Looking forward

Taiwan is not alone in Asia in not "washing one's dirty linen in public." In Taiwan, companies are yet to deal openly with fraud and related issues, the perceived stigma and reputational risk being all too great. Much fraud is also not even detected by companies.

It is therefore difficult to get a real picture of the fraud landscape in Taiwan, and predict how it will look in the near future. However, it is unlikely Taiwanese companies will escape unscathed from global trends of increasing regulation and enforcement of far-reaching antibribery and corruption legislation, as well as the universal threats of cyber crime, intellectual property fraud, and information theft. Until the dialogue begins in Taiwan, and organizations are more transparent and vigorous in pursuing fraudsters, the inside fraudster and the external perpetrator will be on the winning side.

Rex is a recognized authority on investigation of economic crime. As a certified fraud examiner and accredited information system auditor, Rex is a frequent speaker at various forums, and provides investigation training to clients such as the securities and futures institute, R.O.C.

Rex has conducted a number of fraud investigations throughout Asia Pacific, providing specialist IT knowledge and skills. Having conducted compliance reviews of antibribery and corruption legislation, as well as anti–money laundering (AML), Rex assists clients to design and implement appropriate compliance systems, also providing training on AML to clients such as the Bank of Taiwan and the Taiwan authority of financial services.

Thailand

Douglas Webb
Executive Director, Forensic
KPMG in Thailand

- **Multinationals can struggle to effectively oversee their local operations so far from their head office**
- **The high premium on hierarchy and relationships reduces the stigma attached to corruption**
- **Forward-looking companies are developing fraud risk awareness and joining deterrence initiatives**
- **Companies use third parties to try to distance themselves from their bribery and corrupt practices**

We've investigated a number of cases where the fraudster turned out to be the top dog – the head of a relatively small organization – who was able to use his influence and authority to get people to go along with his scheme.

Thailand, in the middle of the Indochina peninsula in Southeast Asia, is uncannily resilient, able to consistently grow at 4–5 percent per year despite recurring interruptions such as the tsunami, flooding, and more recently, political flare-ups. Year after year, Thailand continues to be a preferred tourist destination as well as a leading manufacturer in the region.

Fraud in Thailand fits the global narrative, with the trusted inside person taking advantage of gaps in a company's fraud defenses. The tale of abuse includes employees embezzling or misappropriating company assets, with senior executives committing fewer but more costly financial statement frauds.

"At local companies and multinationals alike, we see the same types of basic fraud schemes occur over and over. What stands out is the lack of controls and the relative ease by which existing controls can be overridden. Once someone is successful at committing fraud, they tend to repeat it until they are caught."

Yet, Thailand offers some unique opportunities for the fraudster. With the world's fastest growth rate prior to the Asian meltdown in 1997, the leading multinationals established a presence in Thailand long ago. Thailand remains home to significant foreign investment particularly in the electronics, auto parts, and manufacturing sectors.

"Multinationals often have relatively small offices in Thailand, meaning few people and little segregation of duties and oversight. Our investigations have shown that this situation can be easily abused, with management and sometimes employees overriding the controls."

Multinational and foreign companies also have few soft controls to compensate for gaps at their small operations in remote locations.

"One of the big issues with foreign operations in Thailand is the problem foreign investors have implementing their head office's anticorruption policies locally, for example, policies on gift giving, travel, entertainment, facilitation payments, and conflicts of interest. Distance, culture, and language all cause interference in the communication of these policies. Even the leading multinationals often fail to communicate their head office policies effectively to their local operations. This has led to some costly investigations."

Thailand reflects many characteristics seen across the Asia Pacific – a high premium on hierarchy and relationships, a paradigm of nonconfrontation, and little stigma attached to corruption.

Investigations in many Asian countries, including Thailand, often reveal that a senior person was able to commit fraud by pressuring more junior staff to assist despite their not benefiting from the crime.

"Even when it's only the executives or senior management who were involved in committing the fraud, we often find that the employees knew about it, but were afraid to speak up."

Global trends show increasing collusion, which is ultimately bad news for companies as fraud involving collusion tends to go on longer and be more costly. Throwing more hard controls at collusion has little effect; the only real defense is to make people aware of the issues, the alternatives, the risks, and the consequences. This is what fraud deterrence tools and practices achieve.

"Thailand does stand out a little from its neighbors in that companies are increasingly interested in fraud risk management. We are helping companies to assess their fraud risks and to identify gaps in their controls, while training their staff in fraud awareness."

While prevention measures like fraud reporting hotlines were uncommon in Thailand five years ago, they are becoming increasingly popular – the trend began with multinationals but has started to spill over to local companies who see hotlines as a cost-effective way to detect and prevent fraud.

Asian companies based in Thailand often deal with allegations of fraud indirectly. Wary of confrontation and the negative effect of an investigation on staff morale, many Asian companies prefer to engage in visible fraud risk management initiatives to address suspicions of fraud. In this way, companies deal with the allegations of misconduct more proactively, changing the company culture and tone, and closing control gaps while sending a strong message to implicated employees and general staff without loss of face.

Thailand has a number of fraud laws on its books, but enforcement is weak. Like most Southeast Asian countries, Thailand currently ranks in the middle to lower end of Transparency International's corruption perception index; with many Japanese, British, and American companies in Thailand, corruption is definitely an agenda item for both foreign and local businesses.

While awareness of antibribery and corruption laws and regulations in Thailand is relatively low, it is improving, partly due to several high-profile U.S. Foreign Corrupt Practices Act (FCPA) investigations. Prompted by an increasingly intolerant public, the private sector is also intensifying its efforts to reject participation in corruption, and improve policies and controls.

"The private sector has started a grassroots initiative to fight participation in corruption. Since 2010, over 200 of the leading companies in Thailand have become signatories to Thailand's Private Sector Collective Action Coalition against Corruption."

Nonetheless, private companies still face challenges with corruption in both their private and public sector interactions. Fraud in procurement, often facilitated by under the table cash payments, can be very hard to identify. The external fraudster is also in the mix, with third parties facilitating bribery and corruption, making it even harder to identify all of the fraud's participants.

"We see situations where companies decide to pay bribes, but then try to distance themselves by using a third party to make the payment."

Multinationals that distribute their products in Thailand through the use of third-party distributors have been caught trying to use these agents or local firms to smooth the way with bribes and payments without the transactions appearing on their own books in hopes of complying with antibribery policies and regulations. Companies may believe this disguise is enough to avoid detection or are simply unaware that "once removed" is no protection.

Theft of corporate data by employees or as a result of cyber crime is increasing as elsewhere, but organizations are definitely behind the curve in recognizing their exposure and preparing for it.

"We have assisted a number of clients recently whose sensitive information, such as customer lists and production secrets, were taken and sold on the gray market. Not all organizations have the controls in place to protect personal data and sensitive company information."

Looking forward

"With greater awareness of fraud through the media, anticorruption campaigns, and visible FCPA prosecutions, we are optimistic that the next generation in Thailand will continue to develop greater levels of intolerance toward fraud."

Douglas leads KPMG's Forensic Service practice covering Thailand, Myanmar, and the Lao PDR. Based in Bangkok, he is actively involved in advising local firms and foreign multinationals operating in the region on fraud investigations, fraud risk management, contract compliance, fraud awareness training, contract disputes, and integrity due diligence

The Offshore Group

Bermuda, Bahamas, Jamaica, Cayman Islands, Turks & Caicos, Anguilla, Barbados, Antigua, Trinidad & Tobago, Malta, Gibraltar, Channel Islands, Isle of Man

Charles Thresh
Managing Director
Regional Head of Forensic
KPMG in Bermuda

- **Cloak of invisibility eroding, with regulated company service providers (CSPs), bank secrecy, and tax haven status under scrutiny**
- **Island jurisdictions ahead of curve on AML compliance but face ongoing public relations challenge**
- **Well-established guidance and enforcement for banks and investment companies, but increasing focus on CSPs, trust companies, and other high value, low volume business**
- **Mobile money may be a game changer for money laundering and the fraud landscape**

It's difficult to overemphasize the impact the international anti–money laundering (AML) lobby has on island jurisdictions. As the financial sector dominates these island economies, there's plenty of focus by government and business on AML enforcement.

In order to focus on the issues and requirements unique to clients in island economies, KPMG formed a subregion that contains 17 jurisdictions – from Malta in the Mediterranean to the Cayman Islands in the Caribbean.

"The diverse territories in our subregion make it impossible to speak about a consistent fraud landscape, but common fraud themes do connect them."

These island jurisdictions are mostly small economies dominated by financial services, tourism, and infrastructure. Many provide financial, legal, and other services to nonresidents on a scale that is incommensurate with the size and financing of its domestic economy. Typically, international banking dominates

these economies, followed by investment funds, reinsurance, and corporate services for international clients. The local economy – often smaller – is about tourism, infrastructure, and on some islands, natural resources.

"Island jurisdictions suffer the same fraud as the onshore world, but historically, the control frameworks are not as sophisticated; however, being heavily reliant on international business, these are strengthening."

Many of these islands have favorable tax regimes for international business and offshore-resident individuals. Some jurisdictions have established their financial sectors by making it easy for foreigners to create legal structures, with the ultimate draw card of bank secrecy laws protecting the identity of customers and their financial dealings. Individual and corporate wealth has been attracted by reduced taxes and lighter touch regulation.

However, extraterritorial regulation, the tax morality debate, and the development of international standards for AML and antiterrorist financing (ATF) have more recently placed all international financial centers under scrutiny. Such centers are now the subject of regular IMF inspections, with these findings made public.

"Many frauds need to recycle ill-gotten gains back into the system. Banks and other institutions are not always involved, but they offer the semblance of legitimate business and are usually somewhere in the transaction cycle."

In short, regulators in the offshore environment have faced a steep learning curve to combat fraudsters, organized crime, and other individuals seeking to benefit from the proceeds of crime, now requiring financial institutions and others to implement controls.

These controls include mechanisms and requirements for reporting suspicious transactions that may be indicative of money laundering, corruption, or terrorist activities.

Certainly, this has led to bank secrecy becoming a hot topic in the regulatory and compliance space. This once sacrosanct business (and legal) principle used to prevent banks from providing customer personal or account details to other parties, even law enforcement agencies, has been put under pressure by the onslaught of the United States and other developed countries chasing tax cheats.

"Generally, most people in the island jurisdictions believe it is more difficult to perpetrate financial fraud than in the past. With local and international regulators so active, people can no longer turn a blind eye to what may have been tolerated in the past."

The wealthier and better established international financial centers believe they are ahead of the curve in AML and ATF compliance when compared to many onshore compatriots. This is in part attributable to their respective financial sectors being more able or willing to bear the costs of compliance. This must surely mean jurisdictions with lower critical mass or more stringent standards than the market is willing to bear will not survive in the long term.

Still, no jurisdiction is immune from the law of large numbers, and huge capital throughput means that instances of wrongdoing occur even in the best regulated environment.

KPMG's experience in the offshore territories indicates that fraud cuts across international and local business, from drugs and procurement fraud to international banking frauds.

Increased involvement of third parties in fraud, frequently in collaboration with insiders, is a global trend, and the island economies are no exception.

"One investigation involved a manager and a supplier colluding by doubling the price on each invoice to split the profit. As the islands are small jurisdictions, collusive relationships are easily developed."

AML/ATF enforcement that started with banks, and has more recently moved to funds and trusts, now extends to Corporate Service Providers (CSPs) – a trend that further erodes the shell company cloak of invisibility as the administrators of these structures become subject to tighter regulation.

At the beginning of 2013, Bermuda introduced the Corporate Service Provider Business Act 2012, initiating a new CSP licensing and supervisory regime that mirrors the global trend of strengthening regulation.

"Investment brokers, like other players in the financial community, have been affected by the economic downturn; as investments did poorly, there was a lot of pressure to hide gaps from poor investment decisions or embezzle to maintain their lifestyle. This has been the basis of at least one business failure we have seen."

Of importance to island economies, however, is that the financial fraudster can look a little different than his or her onshore counterpart. With much of the abuse related to money laundering perpetrated in these cases through third parties, or frauds by owners of investment companies, the offshore fraudster is often the principal behind the company, rather than an employee, service provider, or banking customer, as is usually found onshore.

What the offshore fraudster has in common with fraudsters worldwide is that he or she is usually 30 to 40 years of age and in a position of trust able to abuse opportunities as they arise.

Most organizations in island economies have moved up the AML control curve; however, the focus on AML compliance means many companies have yet to interrogate their fraud risk and manage this particular exposure.

Looking forward

The pace of change in the regulatory environment in island jurisdictions will continue to accelerate, not slow down. However, fraudsters and the perpetrators of financial crime don't stand still either.

"We expect to see mobile technology change not only the way fraud is perpetrated, but also how money laundering takes place."

The mobile money dialogue introduces the idea of mobile money providers other than banks such as mobile network operators being allowed into the financial sector.

This new "digital financial inclusion environment" will have implications for existing fraud and money laundering typologies, so with the escalating threat of easy cyber attack, the picture is unsettling.

"While investigations don't yet show high levels of high-tech fraud or organized cybercrime in offshore markets, global trends make it seem a question of time."

Charles has worked in the professional services environment for more than 24 years. For 19 of these years, Charles has advised clients in London, Australia, and Bermuda primarily on transactional services: restructuring, forensic, corporate finance, and transaction support. Charles leads the regional KPMG Forensic service line, and as a chartered accountant specialized in AML, insolvencies, and forensic-related issues, Charles frequently hosts client seminars on emerging issues in the region.

Turkey

İdil Gürdil
Head of Risk Consulting
KPMG in Turkey

- **Local fraudster most often engaged in theft of company assets, corruption, and counterfeiting**
- **White-collar criminals more efficient and less exposed thanks to technology**
- **Organizations most concerned about fraud risks relating to cloud technologies and mobile money**
- **Turkey lags in efforts to combat corruption with money-laundering facilitating political corruption**

With advancing technology, a company's systems and technology can be easily accessed using any communication device, leaving companies more prone to fraudsters.

While Turkey currently ranks 54 of 176 on the 2012 Transparency International Corruption Perceptions Index, its limited implementation of the Organization for Economic Co-operation and Development (OECD) Anti-Bribery Convention[1] paints a darker picture for the prevalence of bribery and corruption in the country.

Turkey, a party to the Convention since 2000, has yet to implement key elements of the Convention, including introducing corporate liability for the bribery of foreign public officials and effectively enforcing its foreign bribery offense.

Political corruption in Turkey is not only accompanied by bribery and corruption but also money laundering of these illicit gains.

The most dominant fraud themes in Turkey are theft of company assets, corruption, and counterfeiting, usually seen in high-risk sectors like construction, financial services, and healthcare.

> **"In the last few years, the fraudster in Turkey has usually held a senior management position, including C level directors, general managers, and company shareholders."**

KPMG most frequently sees shareholders commit fraud when their company is acquired by a foreign investor. Financial reporting frauds including manipulation of revenue figures has also increased in Turkey in recent times, largely due to aggressive sales budgets and pressure on employees.

Financial crime in Turkey is, however, subject to regulation and enforcement with bodies like the Financial Crimes Investigation Board, and legislation such as the law on prevention of laundering proceeds of crime and the Turkish criminal law.

To combat the fraudster in Turkey, the Financial Crimes Investigation Board is tasked to develop policies, improve legislation, and evaluate suspicious transaction reports.

In Turkey, technology is fast becoming an integral part of most business environments, presenting a massive opportunity for fraudsters.

[1] Convention on Combating Bribery of Foreign Public Officials in International Business Transactions

"Computer and network technologies make it possible for white-collar criminals to operate more efficiently and with less risk; it eases access, effectively lowering barriers for a new generation of fraudsters."

Technology-related fraud is seen most frequently in Turkey in those sectors that use technology as the basis of their business, like banking and telecommunication.

"We find organizations are most concerned about fraud risks related to cloud technologies, online/mobile payment systems, online/ mobile wallets, and ever-evolving fraud schemes around credit cards and falsified transactions."

Looking forward

"Foreign companies that want to stay a step ahead need to carry out in-depth due diligence of business partners before investing in Turkey."

A Turkish company's ability to deter fraudsters in the future will depend largely on whether it is proactive in establishing healthy and effective fraud risk management systems.

İdil is Head of Risk Consulting services in KPMG Turkey with more than 20 years of audit, advisory, and business experience. In particular, İdil has significant experience in forensic services, internal audit, enterprise risk management, financial management, accounting, and audit. Accredited as a certified fraud examiner and certified public accountant, İdil has served on various audit committees such as the Turkish Ethics and Reputation Society and the Corporate Governance Association of Turkey.

United Arab Emirates

Nicholas Cameron
Director,
Forensic
KPMG in the UAE

- **Close-knit communities generally lead to nepotism and intransparency, both common fraud facilitators**
- **Business practice and fraud influenced by cosmopolitan and largely transient labor force**
- **Large, family-owned corporations provide opportunities for fraudsters as governance lags growth**
- **Light disclosure requirements for corporations make counterparty due diligence key for investors**

Efforts are being made to improve corporate governance in the region, but more work and time are needed to change ingrained cultures which often render these improvements ineffective 'paper tigers.' Nepotism is embedded in daily life.

The United Arab Emirates (UAE) mirrors many of the fraud trends in the Middle East, largely driven by culture, evolving corporate governance standards, and massive capital projects in oil and gas as well as construction.

With 7.8 million people, UAE's history and culture has helped define business norms. Like much of Asia and the Middle East, people in the UAE have always focused on relationships – large extended families and close-knit communities. In a business context, this frequently plays out as nepotism – favor for relatives regardless of merit, which is an enabler of fraud and corruption.

Business practice in the UAE is influenced by its cosmopolitan labor force embracing varied social norms and ethics, with foreigners from the subcontinent, Slav countries, and Europe.

Fraud is also marked by a sense of recklessness; much of life is temporary with three quarters of the population from other countries – allowing fraudsters to think of themselves as outsiders and able to make a quick escape.

Sectors like oil and gas and construction expend huge quantities of money on vast capital and infrastructure projects, yet the people dealing with this procurement often earn low salaries in contrast to the obvious wealth on display, especially in Dubai.

While corruption-led procurement fraud is pervasive in the oil and gas sector, the financial services industry also provides fertile ground as large investment flows move in and out of the country.

Government and other trading companies receive and invest funds both locally and abroad. Relatively superficial due diligence around investment transactions in combination with low disclosure requirements for corporations (especially those established in the many free zones in the country) throws up many opportunities for fraud.

KPMG has investigated cases where advisors turn fraudsters by receiving bribes to make particular investment recommendations to their clients, or invest in fraudulent businesses or just pay too high a price.

The UAE was badly hit by the financial crisis in 2007–2010; it influenced the fraud landscape and the fraudster in a number of ways.

"We have investigated a number of cases involving financial statement fraud, largely driven by the financial crisis. Typically, senior managers manipulate results to meet profit targets – performance-linked bonuses being a great motivator for fraud."

The transient UAE workforce adds to this risk as foreign senior managers manipulate their results to make targets and bonuses before returning home, leaving the issue undetected for months, even years.

Although a large part of the UAE workforce is poorly paid, survival rarely appears to motivate fraudsters.

"The more damaging frauds that we investigate are usually committed by someone chasing the trappings of wealth, basically greed."

Add to the cultural mix a dynamic but relatively young corporate environment maturing through the corporate governance curve, and you have abundant opportunity with often little deterrence.

The UAE ranks fairly well on the Transparency International Corruption Perceptions Index – 27 out of 176 countries.[1] It also ranks as 14th most attractive foreign direct investment globally, ahead of Switzerland, South Africa, and Spain.[2]

Recently, the UAE government has driven efforts to improve corporate governance to match international standards, which is an encouraging development; however, these efforts will need time to produce the desired results.

While many organizations, especially quasi-government entities, are required to have fraud risk management programs in place, its effectiveness depends on the quality of implementation. With a heavy focus on profit, UAE companies, especially the family businesses so typical of the region, tend to underinvest in controls and antifraud measures.

The profile of the fraudster in UAE, like elsewhere, varies.

"In financial statement fraud, we typically see general managers or heads of finance. In the case of kick-backs and corruption, procurement staff and project staff are usually involved."

Cybercrime certainly makes its rounds in the UAE, but KPMG investigations still show companies more frequently defrauded by the internal fraudster, often in collusion with a related party. The frauds that feature regularly are procurement fraud, financial statement fraud, and embezzlement.

Looking forward

As investment flows into the UAE with even larger capital projects ahead, the future trends in white-collar crime and corruption depend on the effectiveness of new corporate governance frameworks.

Increased foreign investment, expected in the next few years, is sure to change the fraud landscape and the opportunities for fraud.

"In this environment, counterparty due diligence is a crucial part of any successful investment decision."

In the immediate future, indications show the familiar fraudster continuing to surface and posing the most risk.

Nick is a director in the UAE Forensic Practice and the lead for investigations and anti-bribery & corruption services for KPMG in the Lower Gulf region. As a chartered accountant Nick has specialised in forensic accountancy for the past 12 years, primarily conducting high profile financial investigations into fraud and corruption offences for government and private sector clients in the lower gulf region and the UK. Nick has acted as the Crown's expert accountant in criminal fraud proceedings and has given oral evidence before the Crown Court in the UK both as an expert and as a witness of fact. Prior to joining KPMG Forensic Nick was a Principal Investigator with the Serious Fraud Office; the UK's leading department for investigating and prosecuting serious and complex fraud and corruption.

[1] TI Corruption Perceptions Index 2012
[2] A.T. Kearney Global FDICI Index

United Kingdom

Alex Plavsic
Partner, Fraud Investigation Practice and Head of Forensic
KPMG in the UK

- **Organized crime is on the increase using old-fashioned deception**
- **The internal fraudster continues to be a growing problem in bad times**
- **Cyber attacks increase and are continuing, with proprietary information vulnerable**
- **Companies say they are prepared, but multiple points of attack and priceless company information make for high stakes**

The ultimate defense in today's environment is to ask whether you are doing business with, and through, people you can trust.

UK companies face an ever-increasing array of frauds and fraudsters, from the "opportunistic fraudster," to the cyber attacker and the professional criminal.

Cybercrime and technology fraud are on the rise in the United Kingdom, either as incidents or as threats, with mobile technology providing opportunities to penetrate the company not just to the insider or the lone hacker, but increasingly to organized crime.

Global statistics tell the story: data loss incidents have increased by 40 percent since 2011 largely via hacking, and external data leaks affected more than 160 million people in 2012.[1] The UK government has responded by announcing free "cyber governance" health checks for companies on the FTSE 350 to assess their information security defenses.

At the same time, according to KPMG's fraud barometer, published in the UK biannually,[2] frauds perpetrated by internal employees or insiders rebounded in 2012, accounting for 80 percent of companies' financial losses from fraud. The scams are familiar: identity fraud, procurement fraud, check fraud, and Ponzi schemes. Even in tough times, people appear unwilling to forgo their lifestyles, with KPMG also seeing a rise in smaller financial statement frauds as senior executives manipulate earnings.

"While we have not seen the large high-profile financial statement frauds from past years, we are now dealing with the 2008 to 2010 legacy, when many companies tried to keep bank and other financing lines open by making financial results appear better than they were."

Although professional criminals appeared to be losing the battle towards the end of 2012, the first half of 2013 saw a major increase in activity with reported frauds in the region of £290m, up from £110m in 2012, with supply chain frauds showing a significant increase.[3]

"Organized crime is getting better at extracting money from corporations. In recent months, we have seen a rise in payment diversion fraud, where the fraudster relies on new or relatively naive employees to change vendor payment details to divert payments to offshore destinations."

Professional criminals are not necessarily using sophisticated technology to defraud their victims either, but rather good old-

1 KPMG's data loss barometer in December 2012
2 KPMG fraud barometer: 2012, major fraud cases heard in the UK's Crown courts for cases in excess of £100,000
3 KPMG fraud barometer – June 2013

fashioned dishonesty and deception, and simple, opportunistic fraud. The problem is that the profile of the organized criminal is relatively unknown and it can be hard to tell if they are inside or outside the organization.

In addition, UK companies frequently have to deal with fraudsters from other countries or jurisdictions, where fraud often goes hand in glove with acts of bribery and corruption.

"In the United Kingdom, more than 60 percent of bribery and corruption investigations relate to problems in other jurisdictions. This is not about more or less corruption in different countries, but the fact that the further away from head office you go, the more the message dissipates, especially in the face of significant pressure on people to achieve results."

While it is never easy doing in-country reviews or audits, companies sometimes deal with their operations in foreign jurisdictions with insufficient rigor.

Despite the fraudster being hard at work in the United Kingdom, companies are only really investing in sufficient controls and fraud risk management after a fraud scare or event.

"We see companies today in the nonfinancial sector spending less on controls and fraud risk management. The counterweight is elevated risk; when things go wrong and people need money, in today's economy, they only have one place to go – their employer."

While a company's best defense against the internal fraudster is to put controls in place and encourage an ethical environment, awareness and quality information technology (IT) systems can also reduce opportunities for the organized criminal.

Looking forward

Looking forward, technology and cybercrime will continue to be a hot issue for UK Boards and management.

"Many companies say they have systems in place, but infiltration needs only one or two flaws in the system and years of innovation is lost and stolen by a competitor. You cannot put a price on preventing these lost opportunities."

With better scrutiny and strong enforcement, more cases of bribery and corruption are expected. In this environment, many companies are regarding what may have been the price of doing business as an unacceptable risk.

Government cut-backs may affect enforcement of organized crime, possibly increasing the threat as the risk versus reward equation becomes even more worthwhile for the organized criminal.

It is in this diverse and evolving fraud landscape that it is increasingly crucial for companies to understand the people and organizations they do business with. Traditional due diligence checks done by procurement functions are no longer sufficient as fraudsters become wise to these controls and adapt their schemes. The best defense for companies is to apply an intelligence approach to integrity vetting, using multiple data sets to provide a better picture of a business partner.

Interesting case from the UK Fraud Barometer

Procurement fraud is about more than just financial loss for a company; it can also affect people's lives and therefore have serious operational and reputational consequences for a company. One such case was reported in the 2013 UK Fraud Barometer where a company sold fake bomb detectors to Iraqi authorities, at a financial cost of £55m, but the real damage was human injury and suffering.

Alex Plavsic is head of KPMG Forensic in the United Kingdom and partner in the Fraud Investigation practice. He has 25 years' experience as an accountant, 20 of which have involved investigations of fraud, bribery and corruption, accounting misstatement, asset tracing, and regulatory inquiries. Alex has led the investigation of various high-profile cases including several of bribery and corruption cases where he presented in the United States to the Securities and Exchange Commission and the Department of Justice and in the United Kingdom to the Serious Fraud Office.

United States

Phil Ostwalt
Investigations Service Network Leader, Global Coordinator for Investigations for the Global Forensic practice KPMG in the US

- **Fraud and the fraudster – ever-present and ever-changing**
- **Fraudsters seize the opportunity of the day – today, it is technology**
- **Cyber attacks – a real and present danger for all companies; introducing a new fraudster**
- **Archetypal fraudster finds opportunities in control gaps and areas of low enforcement**
- **Companies slow to adapt compliance programs for new risks from a changing environment**

> The intriguing thing about fraud is that it is always morphing, like a strain of flu – you can cure today's strain but next year it evolves into something as bad if not worse.

The big thing about fraud is that it keeps happening despite companies' best efforts to implement compliance and ethics programs.

Organizations in the United States are still being affected by traditional fraud, although perhaps nuanced to evolving opportunities. Financial frauds of self-dealing, conflict-of-interest, expense claims, and financial statement fraud are still plaguing companies, although technology has changed the how and to what extent.

Increasingly complex technology makes companies vulnerable to unprecedented levels of hi-tech crime.

> **"Undoubtedly, technology is increasingly used to attack company assets – to hack into systems and download intellectual property, obtain a customer list, or critical corporate strategic information either to be resold at a profit or retained for personal gain. This will continue to be a focus area over the next few years."**

KPMG's 2012 cyber vulnerability index for Forbes 2000 companies paints a picture of a world yet to come to terms with the threats posed by cyber attackers. These threats include theft of confidential or proprietary information, disruption of business activities, and financial fraud. Many companies are hacked but fail to realize it, and so have no clear plan to deal with an incident when it occurs.

While the fraudster may present a little differently in today's environment, the fraudster continues to need motivation and opportunity, both provided by the economic downturn, with financial needs and pressure to protect jobs encouraging fraud.

With pressure on earnings targets and budgets, the rise of the "accidental fraudster" highlights the danger of practices that push the limits of prescribed guidelines and bypass boundaries. KPMG investigations show that while earnings manipulation or reporting fraud may start with edgy or creative practices, it quickly evolves into something characterized as fraud.

Technology has created new opportunities, bringing different players into the market.

"Cybercrime brings with it a different type of fraudster: a younger, educated person without corporate experience but having learned the business playing with technology early on. This person has the power to do extensive damage to companies."

Frequently sitting outside of the organization, sometimes colluding with insiders and often not reported or even detected, the profile of the cyber attacker is difficult to pin down. Cyber faces include hackers or script kiddies, "hacktivists" disrupting services for political gain, organized crime intent on financial gain, or governments with political agendas.

The archetypal fraudster continues to feature as lack of enforcement and broken controls still provide opportunity for the insider. Employees and former employees continue to be among the major e-crime risks, reminding companies of the need for internal cyber security controls.

Compliance programs remain critical in deterring, preventing, and responding to fraud.

"While we are incredibly impressed with those multinational organizations that have developed a mature compliance culture, this in no way reflects the position of the majority of companies in the United States. Many Forbes 2000 companies having fallen behind on the compliance curve will need years to catch up."

In some Boardrooms, less attention is given to the control environment than five years ago, suffering from the proverbial Sarbanes-Oxley hangover, and possibly not driving management to the level of fraud risk management seen in the past.

While companies should certainly not be overinvesting in compliance programs, they do need to reach a minimum threshold to match what regulators expect.

"More often than not, companies have to go beyond this minimum threshold, bolstering defenses for specific and changing threats unique to their environments. What drives a company's compliance requirement is what management and Boards have to understand, what takes them beyond the minimum threshold."

Putting a compliance program in place is a beginning and not the end, with management needing to revisit and revise controls as fraud and the fraudster continue to morph.

"Companies can't stand still to allow yesterday's controls to address today's or tomorrow's fraudster."

Companies are building defenses against the cyber-criminal, with few keeping pace with the evolution from stand-alone hacker to insider and organized crime. Top management is still getting to grips with layered defenses going beyond technology to the human element, all the while decoding a foreign expertise to navigate the way forward.

"While some sectors are better prepared for cybercrime than others, companies that have experienced high-profile cyber incidents do not necessarily appear in a better position to deal with future attacks. These companies are also struggling with how to manage this risk proactively."

Looking forward

The future profile of the fraudster will largely be determined by the prevalence of cybercrime, as well as changing technology and enforcement.

The conditions over the past few years have been ripe for financial statement fraud, with economy, control gaps, and less enforcement. With signals from the U.S. Securities and Exchange Commission suggesting a greater focus on this area, more financial statement fraud may well be seen in the immediate future featuring the senior manager or executive.

"Ultimately, however, the fraudster of tomorrow will depend on the opportunities of the day."

Phil Ostwalt is a partner in KPMG Forensic with over 28 years' accounting and advisory services experience with public accounting firms and in private industry. Phil specializes in forensic accounting and investigation services. He has conducted an extensive number of financial, accounting, and regulatory investigations on behalf of public and private companies, organizations, audit committees, special committees, and their counsel.

Vietnam

John Ditty
Chairman, Vietnam and Cambodia Managing Partner – Advisory KPMG Limited in Vietnam

- **Economic outlook pushes local tolerance of bribery and corruption to tipping point**
- **Limited credit combined with pressure for results and targets drives financial statement fraud**
- **Carte blanche for internal fraudsters being withdrawn as companies turn to controls in hard times**
- **Increasing awareness of clean business imperative for investment**

Investment is linked to the strength of financial institutions and the quality of governance. Having a company code of conduct to set ethical standards and promote a culture of clean business is not just about fraud deterrence; it's a long-term growth imperative.

Vietnam, a communist state home to 90 million people on the Indochina Peninsula in Southeast Asia, is waiting to catch its second wave.

Foreign investors once lured by the world's fastest growth rate have been pulling back. Despite being relatively unaffected by the global crisis, Vietnam's economy has stalled affected by many domestic issues.

Vietnam's fraud landscape is closely intertwined with its economic narrative – one of the issues facing foreign investors is the difficulty of doing business in Vietnam due to endemic bribery, corruption, and fraud.

Although Vietnam ranks 123 out of 176 countries on Transparency International Corruption Index,[1] one of the more corrupt countries in the world facing big challenges in clean business and governance, investors still reference the country's natural advantages and the chance of a second wave.

Despite indications of growing local intolerance and future improvement, fraud is still on the rise with more people under pressure, whether to maintain lifestyle and credit lines or secure investment.

> **"Where a financial controller may have thought about it in the past, he is now so overextended that he is doing it."**

While there is no idée fixe for the fraudster in Vietnam, KPMG investigations show the typical fraudster as someone within the organization, the insider, aged between 30 and 45.

[1] Transparency International Corruption Perception Index 2012 – Vietnam ranked 123 out of 176 countries

"Personal factors influence if and when a person turns fraudster. People close to 30 often start reaching for a different lifestyle. We seldom see fraudsters over 45; they get caught or stop."

Culture may be a nebulous concept, but it plays out in fraud. Vietnamese culture, as in other Asian countries, is rooted in relationships, tight-knit communities, and extended family groups, forming the bedrock of social norms like gifts and nepotism. These, when transposed into a business environment, emerge as kickbacks, bribery and corruption, or conflicts of interest.

"Kickbacks and bribes in procurement are widespread, touching many businesses; it is part of how business works in Vietnam, and often considered harmless compared to fraud or theft."

Public and private procurement in Vietnam are characterized by collusion, related parties, and questionable payments. Employees, procurement officers, and managers frequently collude with friends, family, and other related third parties.

"In training sessions to local companies, when we ask whether they have a code of conduct, few raise their hand."

Companies worldwide are strengthening company culture and embedding ethical standards, driven by legislation but also business imperatives. Practically, this means strong codes of conduct linked to conditions of employment, and employees who are aware of ethical norms and fraud issues.

Good governance in procurement includes due diligence of third parties to assess integrity and root out conflicts of interest.

"Carrying out due diligence in Vietnam is challenging due to limited information in the public domain. Employee screening can also be difficult as applicants fabricate credentials."

A typical fraudster in Vietnam is the senior employee, frequently engaged in financial statement fraud, especially in the recent climate. Financial reporting fraud is common, generally prompted by the expectations of external parties, meeting bonus targets, or simply matching bank thresholds to secure or maintain a line of credit.

Vietnam's flat economy with limited credit makes funding competitive. Managers and owners therefore try to paint a rosy picture of their business; some prefer to bribe the bank official.

"It used to be common practice for banks or borrowers to give credit officers a percentage of approved loans, but the number of bad loans written by officials tempted by incentives was becoming an issue."

Companies have cut salaries and increased incentive-based remuneration in many parts of the world. KPMG investigations show this to be driving fraud, not unexpected perhaps given the history of Enron and WorldCom.

Intellectual property fraud in Vietnam is enabled by a culture and tolerance of copyright infringements and piracy, from music to software licensing – part of Asia and the "world of knock-offs."

"Intellectual property fraud, information theft, and high-tech fraud are probably the most underreported frauds in Vietnam, and where the fraud risk is going in the future."

Organizations in Vietnam often have weak controls and governance frameworks shaped by a history of business governed by relationships.

"In good times, companies lost money to insider fraud and theft, with money literally walking out of the factory. Now with single growth figures, each dollar counts, so management is focusing on controls."

Government and society have signaled an approaching fork in the road; local companies are relooking at their control and governance structures. The discussion on fighting fraud and corruption has moved from why to how.

Many foreign investors are required to comply with internationally applicable antibribery and corruption legislation, like the U.S. Foreign Corrupt Practices Act and the UK Bribery Act. The risk of bribery and corruption is now a bigger part of the investment decision.

"In our experience, the right kind of controls and antifraud measures not only reduce future losses, but also instill confidence in governance attracting investors."

Looking forward

"We expect tangible outcomes in the next three to five years from the increased emphasis on reducing fraud. With a younger generation under pressure, we may well see a younger fraudster."

John has been living and working in Vietnam since 1993; he is the chairman of KPMG in Vietnam and Cambodia. John's responsibilities include overall responsibility for the Advisory practice of KPMG and he is also the Risk Management partner for the firm. John holds a CPA and has significant experience in emerging markets. In addition to Vietnam and Cambodia, John has worked in Australia, England, Hungary, Laos, and Poland. John has extensive experience in managing and coordinating numerous audit and advisory assignments in Vietnam and Cambodia. He has assisted numerous foreign investors enter the Vietnamese and Cambodian markets and, through his experience, he has developed a wealth of knowledge and understanding regarding business and business practices in Indochina.

Acknowledgements

We would like to acknowledge the following individuals for their assistance:

Elizabeth Cain

Nigel Holloway

Alecia Hope

Victoria Malloy

Theresa Mayer

Lissa Mitchell

Ron Plesco

Kajen Subramoney

Tracey Walker

Estelle Wickham

Notes

Notes

Notes

Contact us

KPMG's Global Forensic Regional Leadership

Petrus Marais
Global Forensic Leader
T: +27 795159469
E: petrus.marais@kpmg.co.za

Richard H. Girgenti
Americas Region Forensic Leader
T: 212 872 6953
E: rgirgenti@kpmg.com

Jack DeRaad
EMA Region Forensic Leader
T: +31206 567774
E: deraad.jack@kpmg.nl

Grant Jamieson
AsPAC Region Forensic Leader
T: +85 221402804
E: grant.jamieson@kpmg.com

KPMG's Global Forensic Investigations Network

Phillip Ostwalt
Global & Americas Investigations Leader
T: 404 222 3327
E: postwalt@kpmg.com

Dean Friedman
EMA Investigations Leader
T: +27 116478033
E: dean.friedman@kpmg.co.za

Mark Leishman
AsPAC Investigations Leader
T: +61 7 3233 9683
E: mleishman@kpmg.com.au

kpmg.com/fraudster

kpmg.com/socialmedia

kpmg.com/app

Download on the App Store

Designed by Evalueserve.

Publication name: Global profiles of the fraudster

Publication number: 130686

Publication date: November 2013