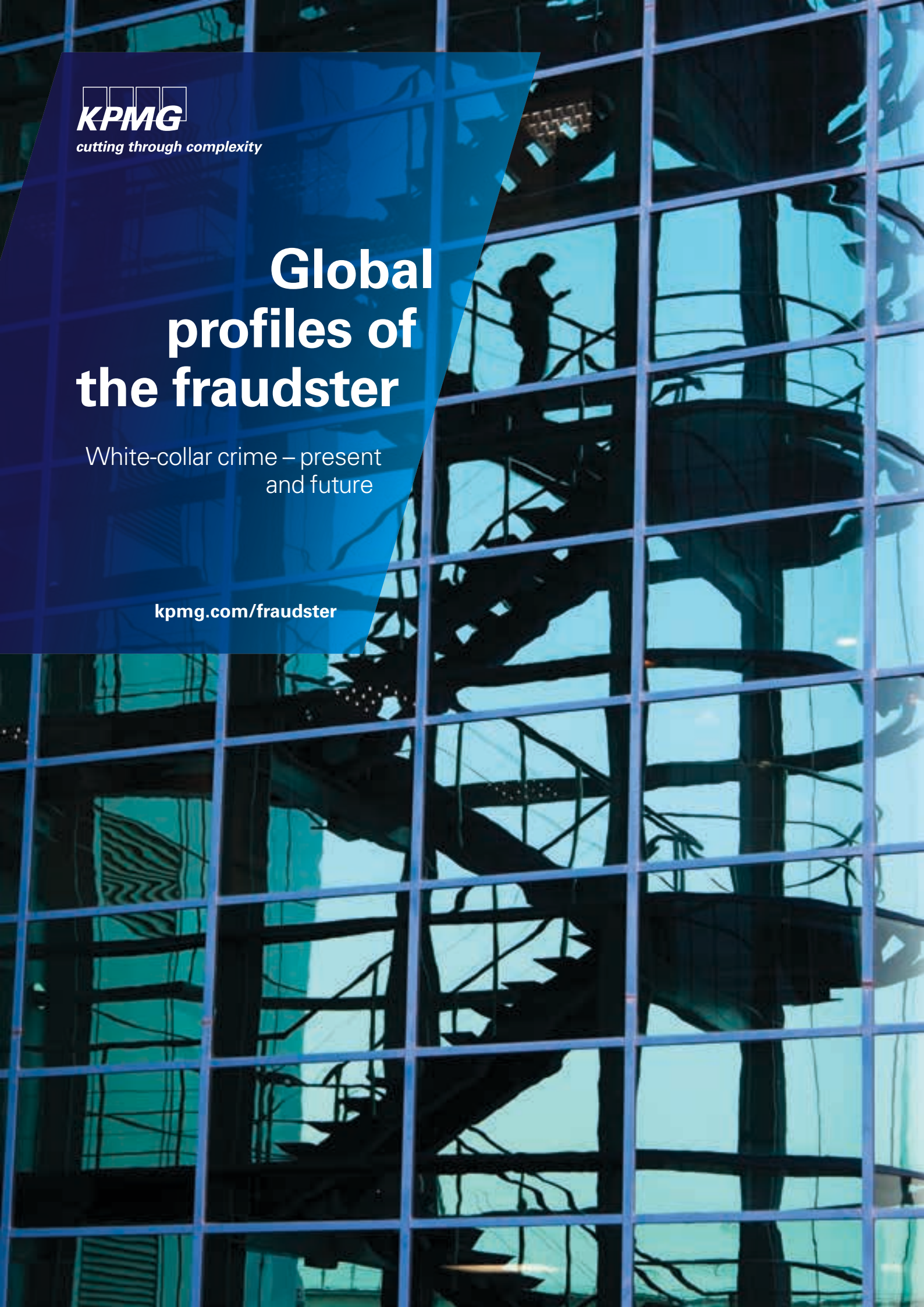


KPMG
cutting through complexity

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

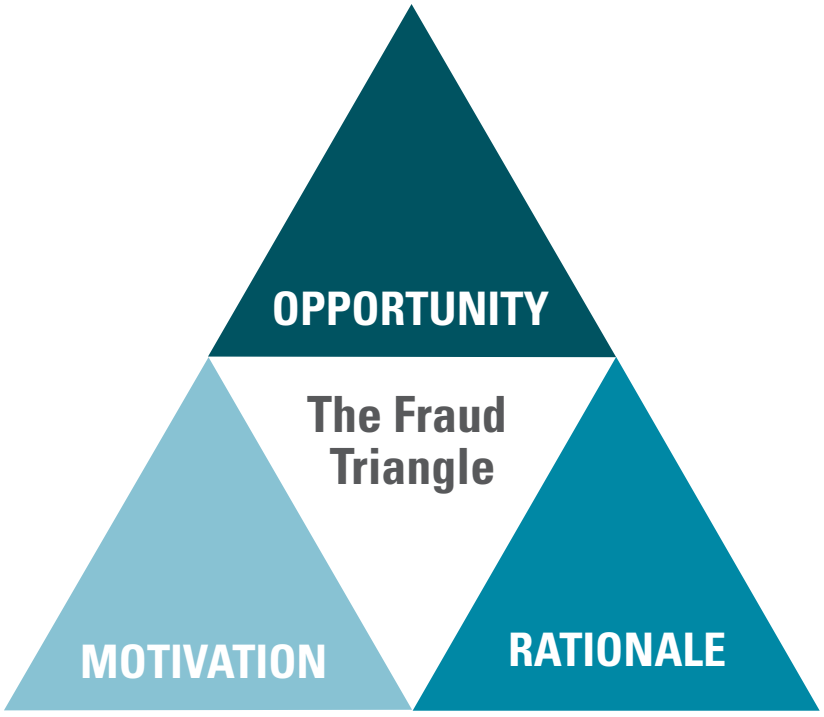
The findings in this report are contrasted, where possible, with our 2007 and 2011 analysis to highlight shifts in patterns and to provide a perspective on emerging trends.

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.

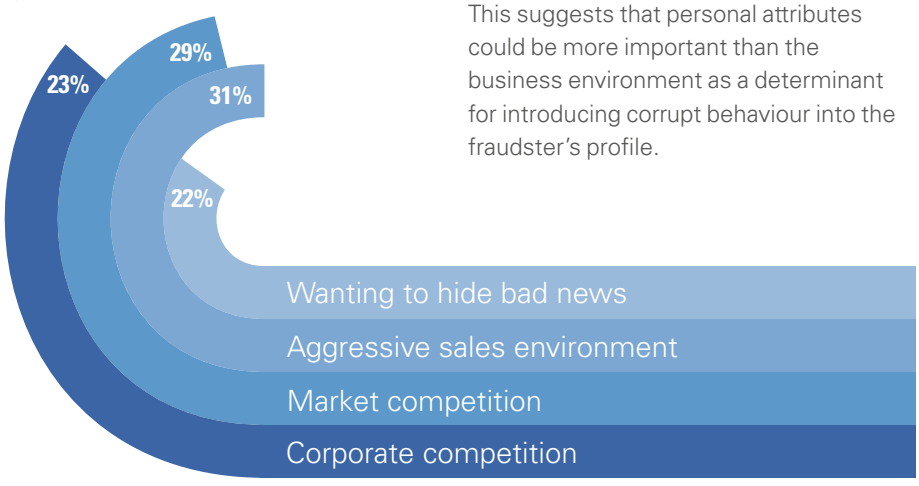
Phil Ostwalt
Global Coordinator for Investigations for the Global Forensic practice at KPMG.

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.

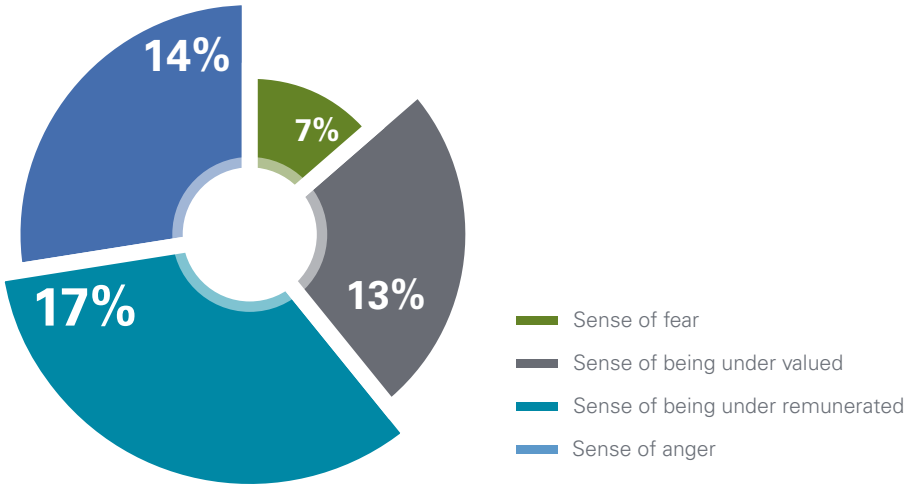
Personality and capability

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



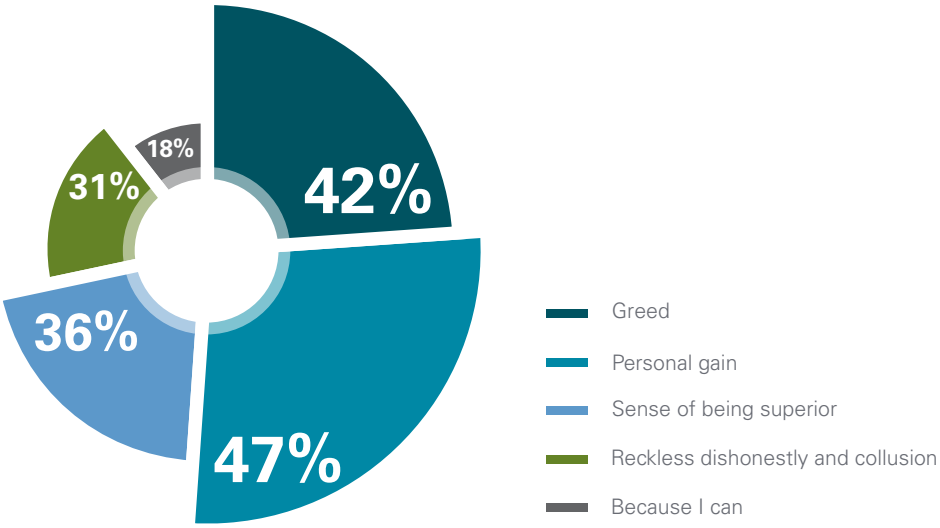
Source: Global profiles of a fraudster, KPMG International, 2013.

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.

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

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