KPMG

Global profiles of the fraudster:

Technology enables and weak controls fuel the fraud

May 2016

kpmg.com/fraudster

KPMG International





Content

Foreword

Fraud is a global scourge that harms corporate reputations, costs millions and ruins lives. It is a heavy economic and moral burden on society. KPMG has reported on fraud trends for many years and this is the third report that profiles fraudsters around the world. For this report, our professionals completed a detailed questionnaire about 750 fraudsters, based on what we learned during our investigations.

We added new questions in the third survey to learn more about the types of people who commit fraud, the sorts of fraud they commit and the manner in which the frauds are detected. The latest questionnaire included queries regarding the technology component of fraud and cyber fraud. We conclude this report with our recommendations as to how best to combat fraud in an environment where the threats are evolving.

This report on the profile of the fraudster is intended to help clients to understand this complex field and how it is likely to change in the future. We also hope our survey will contribute to a worldwide discussion about fraudsters and ways to combat them. Companies, governments and society at large have a direct interest in the outcome of this discussion.

Petrus Marais
Global Head of Forensic
KPMG International

Phillip Ostwalt
Global Head of Investigations
KPMG International

Executive summary

— Anti-fraud controls (such as internal audit, suspicious managers and co-workers, and anti-fraud processes) are not strong enough, and the problem is growing. KPMG's survey of 750 fraudsters worldwide found that weak internal controls were a contributing factor in no less than three quarters of them. There was a sizeable jump in the proportion of fraudsters who saw an opportunity that presented itself due to weak controls, compared with the previous survey in 2013.

— Even if controls are strong, fraudsters evade them or override them. Different forms of detection come into play (such as whistle blowers, other kinds of tip-off mechanisms, and suspicious customers and vendors), especially to check executives with too much power.

— Fraud is almost twice as likely to be perpetrated in groups as in solitude. This is partly because fraudsters need to collude to circumvent controls. So collusion is especially threatening for a company. Larger groups (say, five or more people) tend to do more harm financially than single fraudsters or small groups.

— Male fraudsters tend to collude more than women do. They outnumber women almost five to one in the survey, though the proportion of women has risen since 2010. Male fraudsters also tend to be more senior than women in the organization.

— Groups of fraudsters very often comprise people both inside and outside the company. Sixty-one percent of colluders are either not employees of the company, or are employees who work with people who aren't. Some of them are former employees. This highlights the need for better third-party due diligence of such persons as vendors and customers.

— Technology helps both the fraudster and the company combatting fraud. Almost a quarter of fraudsters rely on technology. Companies, by contrast, could do a great deal more to use technology as a tool to prevent, detect and respond to wrongdoing. The key anti-fraud technology is data analytics, a tool that can sift through millions of transactions, looking for suspicious items. But only 3 percent used pro-active anti-fraud data analytics in detection of the fraudsters surveyed.

— Cyber fraud, an important form of technology-based fraud, is emerging as a growing threat and many companies are aware of the issue but seem to be doing little about it.

— Fraud threats are constantly changing and companies need to conduct regular risk assessments, altering the way they prevent and detect fraud, as needed.

The profile of fraudster

Based on a worldwide survey of KPMG professionals who investigated 750 fraudsters between March 2013 and August 2015, the typical fraudster has similar characteristics when compared to the KPMG surveys completed in 2013 and 2010. Consistently across the KPMG surveys, the perpetrator of fraud tends to be male between the ages of 36 and 55, working with the victim organization for more than six years, and holding an executive position in operations, finance or general management. Additional key characteristics of the fraudster revealed in the 2015 survey are as follows:

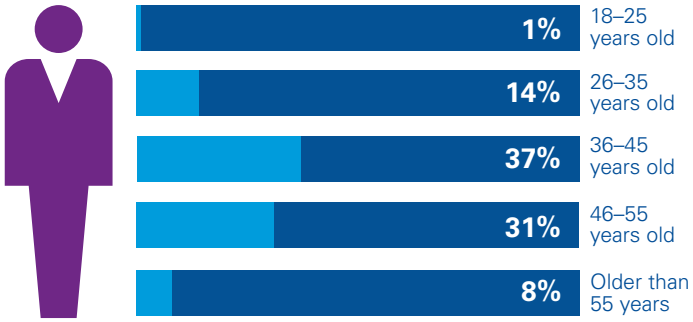
Gender and Age

— 79 percent of fraudsters are men; the proportion of women has risen to 17 percent from 13 percent in 2010.

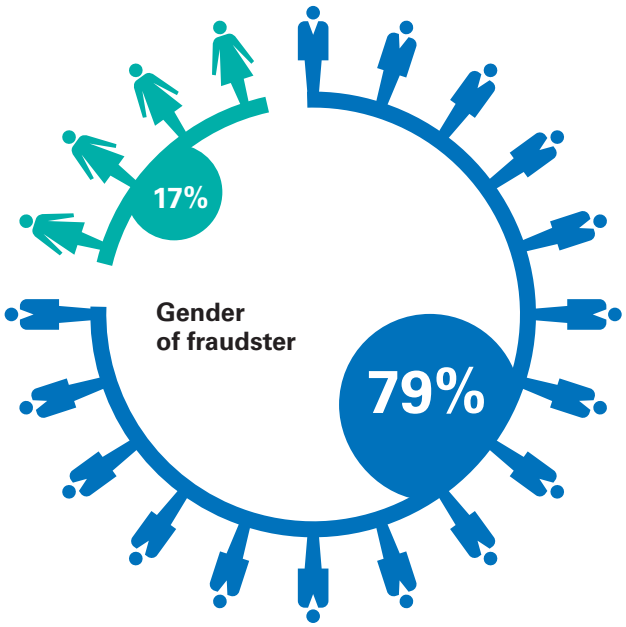
— 68 percent of perpetrators (male and female) are between the ages of 36 and 55, almost exactly the same as in the previous survey, published in 2013. Forty-five percent of women fraudsters, the largest cohort, fall in the 36-to-45 age group.

— 14 percent of fraudsters are in the 26-to-35 age group, up from 12 percent in 2010. The proportion of women in this age group declined from 24 percent in 2010 to 19 percent in 2015. The proportion for their male counterparts increased from 9 percent to 13 percent over the same period.

Age of the fraudster



*The age of the remainder is unknown
Source: Global Profiles of the Fraudster, KPMG International, 2016



*Remainder unknown gender
Source: Global Profiles of the Fraudster, KPMG International, 2016

Insiders, Outsiders and Collusion

— 65 percent of fraudsters are employed by the victim organization and a further 21 percent are former employees. Among fraudsters who were employees, 38 percent worked at the organization for more than six years. These proportions did not change from the survey results in 2013.

— In 62 percent of frauds, the perpetrator colluded with others. According to the 2013 survey, 70 percent of fraudsters colluded.

— Women were less likely to collude: only 45 percent of the females colluded with others compared to 66 percent of males.

— Collusion involving more than five people increased from 9 percent in 2010 to 20 percent in 2015.

— Collusion is highest in Latin America and the Caribbean at 76 percent, and Africa and the Middle East at 74 percent. Oceania (Australia and New Zealand) and North America (the U.S. and Canada) have the highest percentage of fraudsters acting alone, at 65 percent and 58 percent, respectively.

Years of service

Source: Global Profiles of the Fraudster, KPMG International, 2016

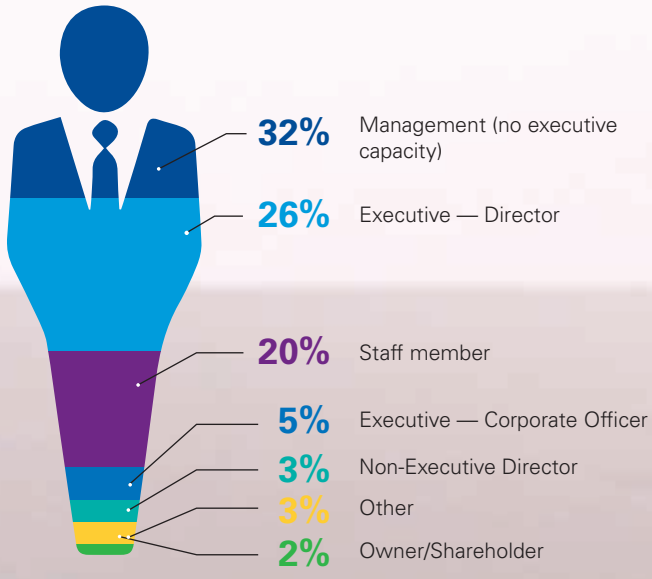
Corporate Title

— 34 percent of fraudsters are executives or non-executive directors; 32 percent are managers and 20 percent are staff members. (In 2013, the respective ratios were 32 percent, 25 percent and 16 percent.)

— 42 percent of female perpetrators are staff members (down from 46 percent in 2010), 38 percent are managers (up from 28 percent in 2010) and 13 percent are executives. Their male counterparts accounted for only 15 percent of fraudsters at the staff level and 32 percent at the managerial level.

— 52 percent of the fraudsters in the Oceania region were at the staff level, in Africa and the Middle East 47 percent were at the managerial level (compared to 33 percent at this same level in North America), and in Europe 39 percent of the fraudsters were at the director level.

Level of seniority



Source: Global Profiles of the Fraudster, KPMG International, 2016

Personal Traits

— 38 percent of fraudsters are perceived to be well respected and 10 percent are of low repute.

— Their sense of superiority is stronger than their sense of fear or anger.

Circumvention of Controls

— Weak internal controls were a contributing factor for 61 percent of fraudsters, compared with 54 percent in 2013. The study indicated that in Europe, 72 percent of the fraudsters said that weak internal controls presented an opportunity for the fraud. Similarly, 59 percent of the respondents in North America and Oceania pointed to this opportunity.

— 44 percent of perpetrators have unlimited authority in their company and are able to override controls.

Characteristics of Fraud

— Technology was a significant enabler for 24 percent of the fraudsters and for the first time our survey includes 31 cyber fraudsters investigated by KPMG

— The most-prevalent fraud surveyed is the misappropriation of assets (47 percent), which is mainly embezzlement and procurement fraud. The second most-prevalent is fraudulent financial reporting (22 percent).

— 24 percent of the frauds in Africa and the Middle East are in the energy and natural resources sector, while 26 percent in Oceania are in the public sector.

— 66 percent of frauds were perpetrated over one to five years (72 percent in 2013) and 27 percent cost the company US$1 million or more, little changed from 2013.

— 44 percent of fraudsters were detected as a result of a tip, complaint, or formal whistle blowing hotline; a further 22 percent were detected as a result of a management review.

Weak controls are a large and growing problem

Corporate fraud is a persistent, global challenge for executives and board members. Managing the risk of fraud has grown more complex as companies face an escalating threat of cyber fraud and no let-up in the more traditional forms of wrongdoing, such as the falsification of books and records. In response, many companies have set up strong internal controls to prevent, detect and respond to fraud. But this is far from universal, as our survey shows that weak internal controls were a factor for 61 percent of fraudsters (72 percent in Europe).

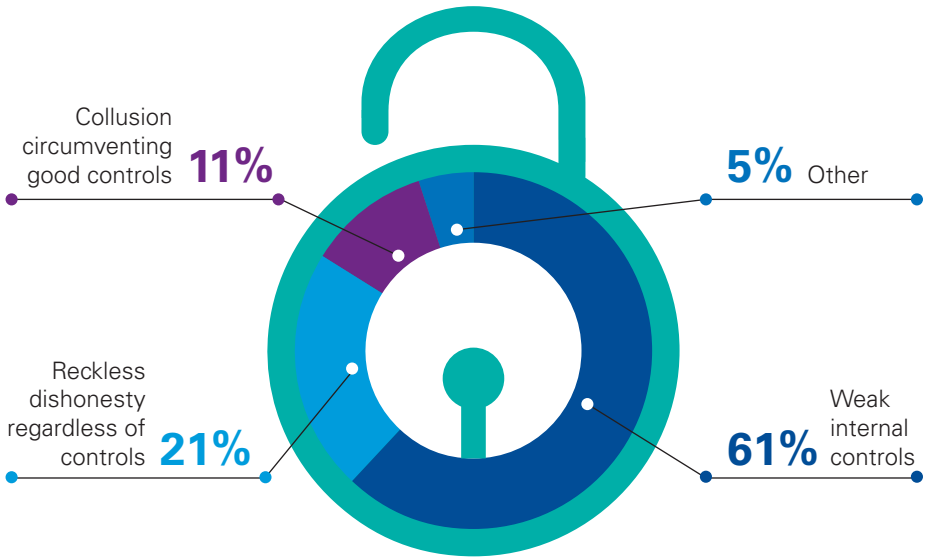
This highlights not only the scale of the management challenge for many companies, but also the potential benefits derived from tightening anti-fraud controls, including the avoidance of financial loss and reputational costs of fraud. Simply put, fraud is less likely to occur in companies where there are robust internal controls and monitoring. "Internal controls are weak when they are poorly designed and are not followed by employees. A thorough fraud risk assessment is likely to show where the gaps are," says Lem Chin Kok, Head of KPMG Forensic, KPMG in Singapore.

This point is reflected in the fact that a significant number of fraudsters (14 percent) were detected by accident rather than by internal controls and monitoring. In 61 percent of the fraudsters surveyed, weak internal controls were a contributing factor in allowing the fraud to occur and go undetected. There are certain controls and processes that are particularly effective in combatting fraud and we will explain what they are in the recommendations section.

Weak controls are a significant issue for companies victimized by fraud and the problem is growing. Compared with 2013, there was a big jump, from 18 percent to 27 percent, in the number of fraudsters who committed (or who appeared to commit) their acts because an opportunity presented itself due to weak controls or a lack thereof. "We have noted instances of fraud where the fraudster's colleagues were aware that something untoward was going on, yet they simply looked the other way. In other cases, colleagues facilitated the crime without knowing it by 'helping out' a fellow employee in a way that actually circumvented the internal controls," says Shelley Hayes, Forensic Service Line Leader, KPMG in Mexico.

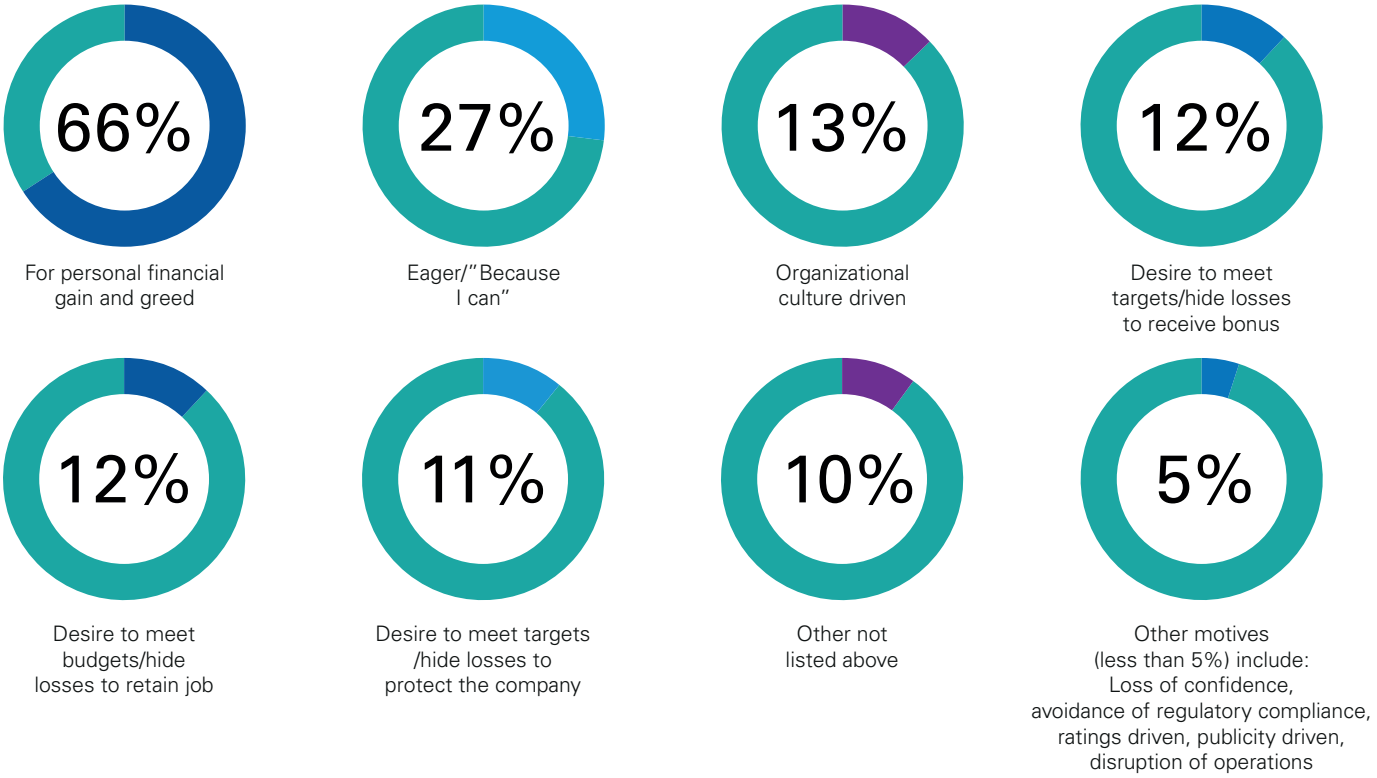
> Internal controls are weak when they are poorly designed and are not followed by employees. A thorough fraud risk assessment is likely to show where the gaps are.

Factors contributing to the facilitation of the fraud



Source: Global Profiles of the Fraudster, KPMG International, 2016

What was the overriding motivation for fraudster?



Unusual features of corruption

KPMG professionals often note that fraud and corruption go hand-in-hand and that regulators around the world are increasingly focusing on anti-bribery and corruption controls. Of the 750 surveyed, there were 125 perpetrators of corruption-type fraud, and they exhibit features that are different from other forms of fraudulent activity. One is that corruption tends to operate at a higher level in a company: 51 percent were executives compared with 31 percent for other types of fraud. And it tends to be concentrated in the office of the chief executive (26 percent compared with 15 percent for other types).

Sixty-three percent of fraudsters engaged in corrupt practices for three years or more, compared with 47 percent for other types of fraudster, but the cost of the fraud was about the same. Corruption, however, was detected in a very different way from other types of fraud. Sixty-one percent were caught as a result of whistle blowers and other kinds of tip-off, compared with 33 percent for other types of fraud. "Reporting of corruption is yet another example of the importance of whistle-blower mechanisms" says Jagvinder Brar, Partner, Forensic, KPMG in India.

Companies understand that fraud is a problem that can lead to financial losses and reputational damage. Regulators around the world are also tightening their supervision of companies and enforcing stricter rules of business conduct, led by the US in the wake of a raft of corporate scandals that have not fully faded from the public's consciousness.

Why is the existence of weak controls a growing problem? One reason found by KPMG professionals around the world is that companies are not investing in stronger anti-fraud controls due to economic hardship. Fraud is increasing in cash-strapped countries such as Greece and Italy, and in distressed sectors, such as energy. When an economy slows down, it is not unusual to uncover fraud that occurred during a time of economic buoyancy, when controls were not rigorously enforced. Another reason weak controls are becoming a growing problem is that companies are venturing into new geographical markets in search of business opportunities, including into countries where corruption is rife.

It appears that cost-constrained businesses and those struggling to grow market share are slow to invest in controls well-suited for their changing risk profiles. "Such companies often eliminate controls without properly assessing the risks of doing so," says Tim Hedley, KPMG Forensic Fraud Risk Management Lead, KPMG in the US. "Regular risk assessments help companies prioritize investments in anti-fraud mechanisms and help to ensure money is spent where it will do the most good."

The biggest frauds override or circumvent controls

We analyzed the 86 fraudsters whose crimes cost the company US$5 million or more. The frauds tended to last a good deal longer than other categories of fraud. They are harder to detect because the fraudsters are more senior than average and involve more collusion, enabling them to circumvent controls. They are also more international. A much higher proportion took place across borders (34 percent compared with 11 percent for lesser frauds).

The fraudsters in this group are generally older than the average. They are 85 percent male and much more likely to involve executives (54 percent versus 31 percent for lesser frauds). "All fraudsters tend to have a sense of superiority, but those committing the biggest frauds tend to be even more autocratic and more frequently to have unlimited authority," says Dean Friedman, KPMG Forensic Head of Investigations, KPMG in South Africa.

This enables them to persuade or coerce others into helping them. Collusion was much more common (86 percent) than among smaller frauds (60 percent) and the colluders are less likely to involve external fraudsters. Almost a third (32 percent versus 18 percent elsewhere) involved more than five people. As one might expect, 51 percent worked in large global firms (compared with 38 percent for less-costly frauds). Twenty percent worked in financial services, versus 8 percent for the rest of the fraudsters.

A particularly pernicious species of fraud is one conducted by groups of five or more, usually males. Twenty-seven percent of the frauds perpetrated by these large groups cost the company US$5 million or more and continue for more than five years. "The most effective methods of detection are anonymous tip-offs and whistle-blowing mechanisms, not internal audit or management review. Fraudsters on steroids are definitely the toughest nut to crack," says Jimmy Helm, Head of Forensic, KPMG Central & Eastern Europe.

People can evade strong controls

Strong anti-fraud controls are important, but they are not a panacea; 21 percent of fraudsters simply were able to disregard the company's controls. They weren't seriously concerned about the possibility of getting caught. Despite the risk of being nabbed, they went ahead and defrauded the company. There are always going to be some people who will take their chances, even if the controls are tight. Some controls appear quite strong on paper, but if they are not strictly followed or simply overridden, the potential for mitigating fraud risk is undermined.

Some fraudsters perceive there is a low risk of getting caught, probably because they occupy powerful positions. They think they can bend or ignore the rules. An extremely high proportion (44 percent) of fraudsters were noted as having unlimited authority. "This poses a double threat to an organization: such people can override controls, weak or strong, and they can order employees to perform tasks to cover their fraud," says Alex Plavsic, Head of Investigations, KPMG in the UK. They also tend to be more damaging: 34 percent of their frauds cost companies US$1 million or more, compared with 18 percent for fraudsters that did not have unlimited authority.

Personal traits can add fuel to the fire. According to the survey, the most frequent description of the fraudsters profiled is autocratic and possessing a sense of superiority perceived to be far stronger than a sense of anger or of fear. Fraudsters with unlimited authority tend to be even more autocratic and have an even stronger sense of superiority.

Outwardly, fraudsters in general are three times as likely to be regarded as friendly as not and are rarely perceived as loners. They tend to be highly respected and don't necessarily have a showy lifestyle. In short, they may not conform to the stereotypical view of how people expect a fraudster to behave.

As we will see in the next section, fraudsters who collude are a particular threat, in part because they evade even strong controls. In companies where anti-fraud mechanisms are tight, 16 percent of fraudsters who collude are able to circumvent them or to persuade other employees to commit the fraud on their behalf.

This analysis does not lend support to the view that it makes no difference whether anti-fraud controls are strong or weak, but quite the opposite. Despite the chinks in the armor, there's been an increase in the proportion of cases where internal controls led to the detection of the fraud (from 68 percent in 2013 to 72 percent in 2015).

What types of mechanisms detected collusion? Of 456 such examples, 52 percent were discovered by means of whistle blowers, other kinds of tips and complaints from suppliers or customers. Other forms of control, such as an internal audit, were much less important, possibly because the company lacked the resources (in terms of manpower or money) for such a function or because the internal audit controls are routine and the fraudster is aware of them. Whistle blowers and tipsters are just as important in detecting fraudsters with unlimited authority.

> "**21 percent of fraudsters** simply were able to disregard the company's controls. They weren't seriously concerned about the possibility."

"This underlines the importance of an effective whistle-blower mechanism supported by the training of all employees on how, why and when to use the mechanism," says Robin Tarr, KPMG Forensic Head of Investigations, KPMG in Australia. But it also suggests that other anti-fraud procedures, such as Internal Audit, need to be strengthened. Companies should ensure that different forms of control are working effectively.

Lone wolves and fraudsters who hunt in packs

For many people, corporate fraudsters conjure up an image of a solitary individual who relies on his or her own ingenuity and cunning to perpetrate the crime. But fraudsters operating in groups are almost twice as common as those going it alone, according to the survey. In 2015, 62 percent of fraudsters colluded with others, compared with 59 percent in 2010. Interestingly, there are marked regional differences in the frequency of collusion. Collusion is particularly common in Latin America and Africa and the Middle East (76 percent and 74 percent respectively). "Fraudsters collude because they need accomplices to evade or override controls or because they lack certain required authority levels, skills and information," says Jack De Raad, Head of Forensic, KPMG in the Netherlands. In contrast, in North America and Oceania we found a disproportionately high number of fraudsters working by themselves (58 percent and 65 percent respectively).

Who are the colluders? Fraudsters who collude tend to be more-senior employees and to have worked longer at the company than the solo fraudsters. Forty percent were executives and non-executive directors, compared with only 28 percent among fraudsters who act alone. It is also striking that only 35 percent of colluders are a purely internal group. The remainder is either a non-employee of the victim company or an employee working with one or more outsiders.

"This shows how vulnerable companies can be to collusion and how they need to design their controls to take account of this, in particular with regard to relationships with third parties, such as vendors and sales representatives," says Graham Murphy, Third Party Risk Management Lead, KPMG in the US. "A strong third party risk management program ensuring the appropriate level of due diligence on suppliers, business partners, and corporate customers is an essential means of vetting and monitoring third parties."

Colluders tend to do a lot more damage than individual fraudsters. Thirty-four percent of collusive fraudsters cost the company US$1 million or more, compared with 16 percent for soloists. Colluders tend to perpetrate larger frauds and escape detection for longer.

> **Whistle blowers (24%)** and **tip-offs (24%)** have the highest incidence of uncovering **groups of five or more colluders.** Other forms of detections may be ineffective in detecting sizeable collusion schemes.

The pattern of detection is quite different also. For solo fraudsters, they are mostly caught as a result of management review, by accident or internal audit. For colluders, the main methods of detection are whistle blowers, management review and anonymous tip-offs. Whistle blowers and tip-offs had by far the highest incidence of uncovering groups of five or more colluders, which suggests that other forms of detection may be ineffective in detecting sizeable collusion schemes.

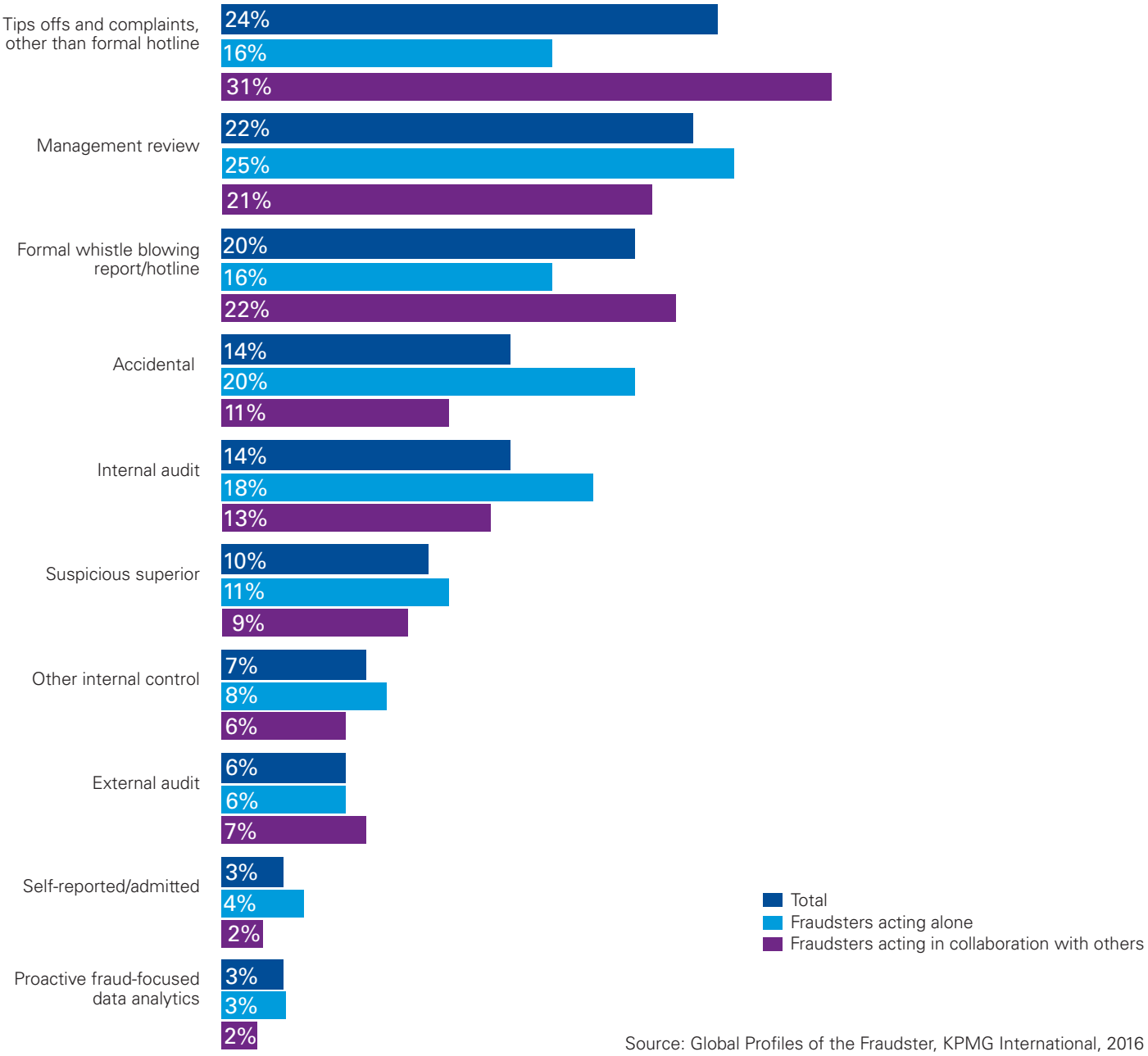
Fraudsters acting alone tend to be more junior than their collusive counterparts. Weak internal controls are a bigger factor for solo fraudsters than colluders (66 percent versus 58 percent). As a result, more are caught by accident than colluders (19 percent versus 10 percent).

When it comes to comparing the sexes, there is a significant disparity in our sample with regard to the tendency to work in groups. Men are more likely to collude than women (66 percent against 45 percent respectively). Women are, however, colluding more than they used to. The proportion of groups that include both genders rose from 34 percent in 2010 to 47 percent in 2015.

It should be noted that men outnumber women approximately five to one in the survey sample, and female fraudsters tend to be more junior in organizations than men. Females are also younger; 63 percent of women are aged 26 to 45, compared with 50 percent of men. And women are more likely to be in financial difficulty than men (14 percent versus 4 percent of the entire sample).

But over time, the differences in fraudulent activity between the sexes have narrowed somewhat, as women rise through the ranks. Female fraudsters were more frequently in management in 2015 compared with 2010 (38 percent vs 28 percent) and the tendency for women to collude has gone up. "The more senior in rank, the greater the ability to persuade others to collude with the fraudster," says Annabel Reoch, KPMG Forensic Anti-Bribery and Corruption Lead, KPMG in the UK.

How the frauds were detected



Source: Global Profiles of the Fraudster, KPMG International, 2016

Internal fraudsters and outsiders

Contrasting solo and collusive fraudsters reveals significant differences. The same is true when comparing collusive fraudsters who are inside the company and those who are outside it. Here the picture is more complex because there are three groups to analyze: purely internal (35 percent), purely external (18 percent) and a combination of the two (43 percent). "Companies have to design anti-fraud mechanisms that look both ways, inside and outside. And they need to be aware of the possibility that a lone, inside fraudster may be working with a sizeable group of people on the outside. There are many permutations organizations must guard against," says Stephan Drolet, Head of KPMG Forensic, KPMG in Canada.

One of the most-striking contrasts in the survey is that the financial harm caused by purely internal fraudsters is greater than either the mixed or the purely external groups. Some 42 percent of frauds perpetrated by this first group resulted in the loss of US$1 million or more, compared with 32 percent and 25 percent respectively for the other two groups. For the purely internal group, there is a much greater incidence of financial reporting fraud than for external and mixed groups (35 percent compared with 16 percent).

There is also a marked difference in the manner of detection. Whistle blowers and tip-offs are a more important means of detection for mixed groups than for purely internal ones (49 percent versus 37 percent respectively).

> "Companies have to design anti-fraud mechanisms that look both ways, inside and outside. And they need to be aware of the possibility that a lone, inside fraudster may be working with a sizeable group of people on the outside. There are many permutations organizations must guard against."

Percentage of frauds resulting in a loss of $1 million or more

42%
of frauds perpetrated by purely internal fraudsters

32%
of frauds perpetrated by groups of internal and external fraudsters

25%
of frauds perpetrated by external fraudsters

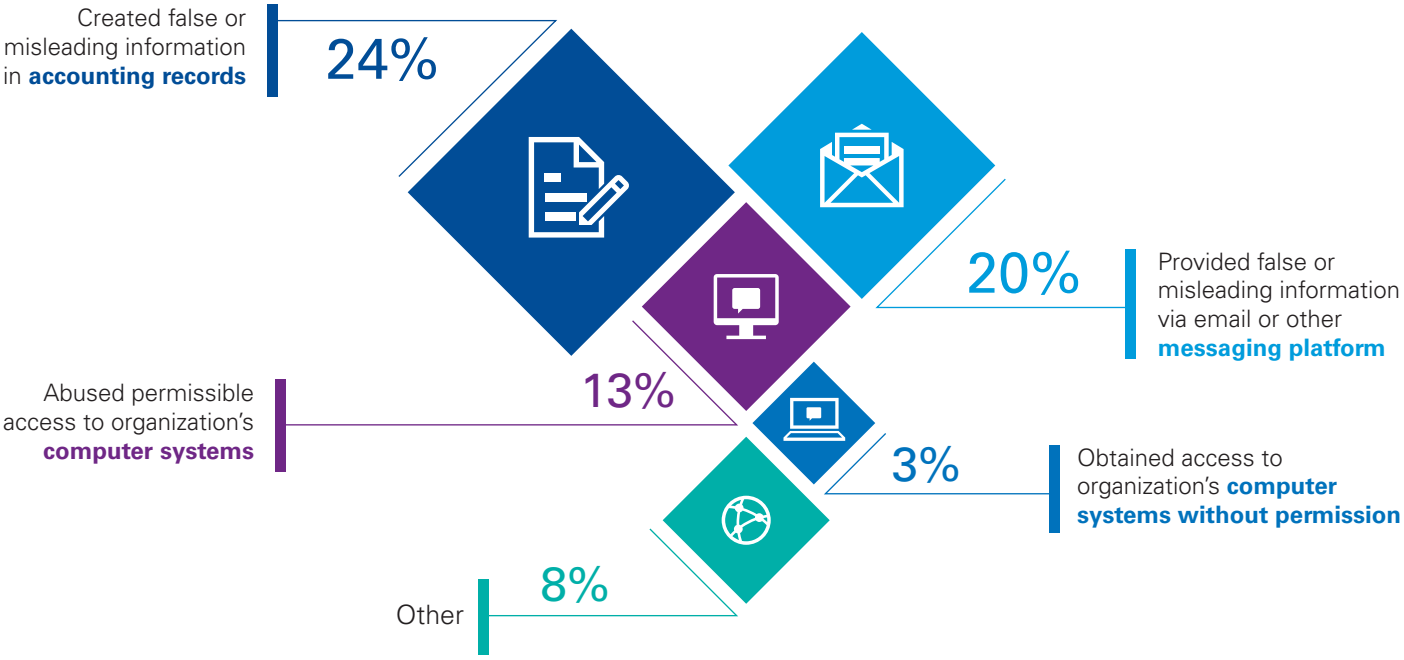
> Companies have to design anti-fraud mechanisms that look both ways, inside and outside. And they need to be aware of the possibility that a lone, inside fraudster may be working with a sizeable group of people on the outside. There are many permutations organizations must guard against.

Technology helps and hinders fraudsters

Technology is a double-edged sword. Technological advances provide more-powerful tools in strengthening companies' defenses against fraud, as well as a means for the fraudster to find areas of vulnerability to penetrate. But our survey suggests that technology is more frequently used in perpetrating fraud than in detecting it. Technology was a major enabler for 24 percent of fraudsters.

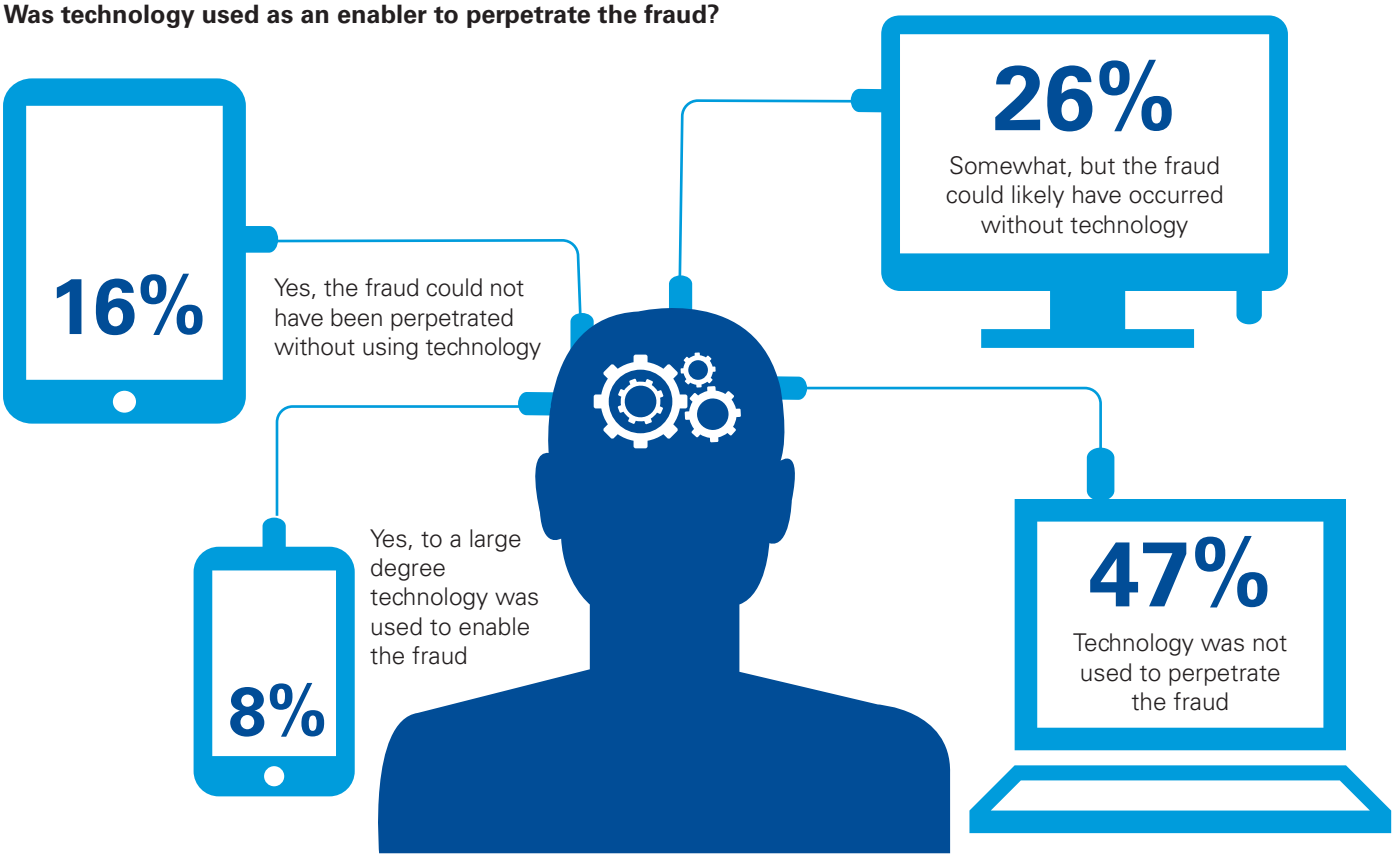
Examples of technology-enabled fraud include: gaining unauthorized electronic access to confidential information, and posting an accounting journal entry to camouflage a misappropriation. Somewhat surprisingly, the proportion of technology-enabled frauds was lowest in Europe (18 percent) and highest in Oceania (30 percent) and North America (29 percent), followed by Africa and the Middle East (28 percent).

How technology was used to perpetrate the fraud



Source: Global Profiles of the Fraudster, KPMG International, 2016

Was technology used as an enabler to perpetrate the fraud?



Source: Global Profiles of the Fraudster, KPMG International, 2016

A very important technological tool in fighting fraud is data analytics, given the size of companies and their geographical diversity. An increasing number of organizations are introducing data analytic solutions to search for unusual transactions amid millions of day-to-day sales and purchases. But data analytics does not appear to be fully deployed by companies. Proactive data analytics, searching for fraud amid anomalies and suspicious business activity, accounts for only 3 percent of frauds detected.

In technology-enabled frauds, the fraudster tends to be younger (60 percent are aged between 26 and 45 years old). "Older fraudsters rely less on technology and more on personal relationships. As younger, tech-savvy employees rise through the ranks, the incidence of technology-related fraud is likely to rise," says Phil Ostwalt, Global Head of Investigations, KPMG in the US. Some 24 percent of technology-enabled frauds were caught accidentally, the most frequent form of detection, compared with 11 percent for frauds not enabled by technology. This provides further evidence that companies could employ technology more forcefully to combat technology-dependent fraud. In some ways, accidental detection is a sobering reminder that the controls are ineffective.

> "Technology is a double-edged sword. Technological advances provide more-powerful tools in strengthening companies' defenses against fraud, as well as a means of finding areas of vulnerability for the fraudster to penetrate."

Cyber fraud is continuing to emerge as a threat

The most frequently cited emerging threat by KPMG offices around the world is cyber fraud. Many noted that companies are aware of the threat but don't think it will happen to them. They therefore may not know they have been attacked and, in any case, this signifies a lack of preparedness against the threat. "We find that executives know that hackers and criminal organizations can wreak havoc on companies; they read about such cases almost every day in the media. But they often don't believe it can happen to them, whether or not they have built defenses against the threat," says Ron Plesco, Cyber Investigations Lead, KPMG Cyber, KPMG in the US.

KPMG survey samples included 31 recent perpetrators of cyber fraud, but this may be the tip of the iceberg. A lot may be going undetected. After all, cyber security has only come into public view in the past couple of years, although it has been going on under the radar for a lot longer.

Thirty-one may seem a small number in relation to the overall sample of 750, but the results are still interesting. The single largest portion (13 people) consisted of employees of the victim's organization, often working with outside syndicates. Nine were associated with organized criminal groups and seven were individual criminals, hacking from outside.

The survey reveals that the main objectives of cyber fraud are the theft of personal data and intellectual property, senior executives' emails, strategic access to company data, and denial of services. The Federal Bureau of Investigation of the US says[1] that there has been a sharp increase in "business email crime", with more than 12,000 victims affected globally. The scam occurs when a criminal sends an email purporting to be from a senior executive and directs an employee to wire money to an overseas bank account. The FBI says it cost businesses about US$1.2 billion in 2013-2015.

"Many companies lack the skills to defend against cyber fraud, so strong internal controls and data analytics are needed. And companies need to share insights with other companies to stay on top of a fast-changing threat landscape" says Kevvie Fowler, Partner, National Cyber Response Leader, KPMG in Canada.

1 http://www.ic3.gov/media/2015/150827-1.aspx

> We find that executives know that hackers and criminal organizations can wreak havoc on companies; they read about such cases almost every day in the media. But they often don't believe it can happen to them, whether or not they have built defenses against the threat.

How to combat fraud

This report provides the main findings of a survey of KPMG investigators around the world, based on their answers to questionnaires regarding 750 fraudsters. The question for companies is how should they combat fraudsters? Based on the analysis of the data, four main recommendations emerge:

Fight back with technology — Our survey reveals that a significant number of fraudsters use technology to perpetuate a fraud. But we could find little evidence that companies are using technology to combat the fraudster. KPMG firms recommend that companies adopt anti-fraud analytic solutions, carefully weighing the cost against the benefit. In effect, they should fight fire with fire. The use of threat-monitoring systems and data analytics is increasing and can highlight anomalous or suspicious behavior by monitoring personal behavior, analyzing computer usage, public records and social media.

Companies are often eager to reap the potential benefits of data analytics and its ability to sift through huge amounts of information they accumulate. But they often buy off-the-shelf solutions that do not integrate well and are eventually scrapped. Far better to look for a more comprehensive solution that will cover most of a company's important surveillance and detection needs. They may even have the software solutions in their existing systems. Alternatively, it may be more effective to export data to a third-party provider. Either way, it is efficient in the long run to conduct surveillance and monitoring continuously by means of automated computer programs, keeping a watchful eye on all transactions every second of the day around the world.

Stay sharp and assess risks regularly — Business is rapidly evolving and fraudsters are always trying to take advantage of the changes to outsmart the system. New regulations, new markets and new technologies are all opportunities for the fraudster to evade controls. How can companies hope to keep up? One of the best mechanisms to defend against emerging fraud risks is a regular fraud risk assessment, conducted as part of an enterprise-wide risk assessment process. Such formal assessments should be conducted annually and updated more frequently, if necessary, to take account of any significant changes in the company's legal environment and business operations. It is a wise, initial step, to stress-test the company's environment (in terms of activity-based controls and entity-level controls), especially when companies engage a group of risk, operations, compliance, legal and other professionals.

Recommendations:

Source: Global Profiles of the Fraudster, KPMG International, 2016

Cyber security assessments may, if the company so chooses, be done separately, but they should be integrated into the overall fraud risk assessment. Given the speed of change in cyber security, it is vital to compare experiences with companies facing similar threats, usually organizations in the same industry.

Know your business partners and third parties — Companies must not only look inward when it comes to fraud, they must also closely monitor their business partners and other third parties that are conducting business on their behalf. As companies extend their reach across the globe, they are increasingly reliant upon these third parties who act as distributors, sales agents, and local country representatives. Conducting risk-rated due diligence at the time of entering into a business relationship is a best practice, and a core element of leading compliance programs.

Furthermore, companies should, from time to time, ensure their suppliers are billing them as per their contractual agreement and they should use their right to audit clause normally included in such agreement. Technology has enabled companies to conduct cost-efficient due diligence, not only at the outset of the agreement, but also to audit a supplier's on-going compliance to a contractual agreement.

Be vigilant against internal threats — A consistently surprising result in our survey is the number of fraudsters who are a senior manager, who has been with the company for at least six years. We frequently hear that "they were the last person we would expect to do something like this." But there are often tell-tale signs. Fraudsters can slip up. If things don't look right, stop, pause and consider. It is essential to develop a strong culture in which employees are aware of the risks of fraud and understand how to respond. Encourage and train employees to use the company's reporting mechanisms, such as a hotline. Nurture a climate of trust in which staff members won't fear for their job if they raise a red flag. Once an alarm is sounded, take appropriate action to inquire or investigate the activity.

These steps will not, by themselves, put a stop to fraudsters; fraud is an elusive and cunning enemy that requires a risk-aware culture to keep it in abeyance. When every employee and every business partner are vigilant and do business with integrity, fraud will subside. It is an objective worth aiming for.

Methodology

The survey is based on a questionnaire asking KPMG forensic professionals around the world for details about the fraudsters who were investigated between March 2013 and August 2015. The professionals filled in a detailed questionnaire on each fraudster, after investigating the case at the invitation of the company affected. The investigation frequently involved interviewing the fraudster, helping KPMG to form a detailed picture of the perpetrator and the fraud committed.

This report is based on an analysis of 750 fraudsters, not fraud cases (some cases involved more than one fraudster). In 2013, the total was 596 and in 2010 it was 348. The frauds in the 2015 survey occurred in 81 countries (including Hong Kong and Puerto Rico)

*percentages may differ by 1 percent due to rounding.

Acknowledgements

Masako Asaka
Jagvinder Brar
Sandra Cusato
Nick D'Ambrosio
Matt Dixon
Laura Dobrotka
Stephan Drolet
Déan Friedman
Renee Gooden
Matt Hansen
Shelley Hayes
Jimmy Helm
Muhammad Hoosain
Tom Keegan
Victoria Malloy
Jack Martin
Kemi Okhumale
Kajen Subramoney
Daniel Viray
Tracey Walker
Estelle Wickham

Contact us

Nicolas Cameron
Head of Forensics
T: +971 44 248 992
E: nicholascameron@kpmg.com

Obaid Kazmi
Director, Forensics
T: +971 24 014 837
E: okazmi1@kpmg.com

kpmg.com/app

Download on the App Store

Designed by Evalueserve.
Publication name: Global profiles of the fraudster
Publication number: 133426-G
Publication date: May 2016