KPMG

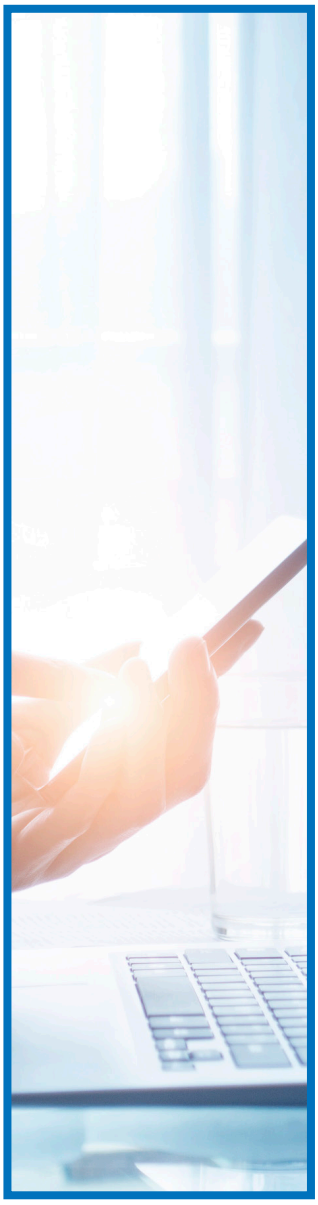
Global profiles of the fraudster

Technology enables and weak controls fuel the fraud

The Indian context

June 2016

www.kpmg.com/IN

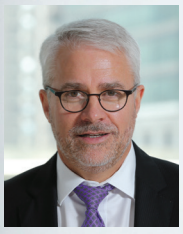

Content

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. Organisations, governments and society at large have a direct interest in the outcome of this discussion.



Petrus Marais
Global Head of Forensic
KPMG International

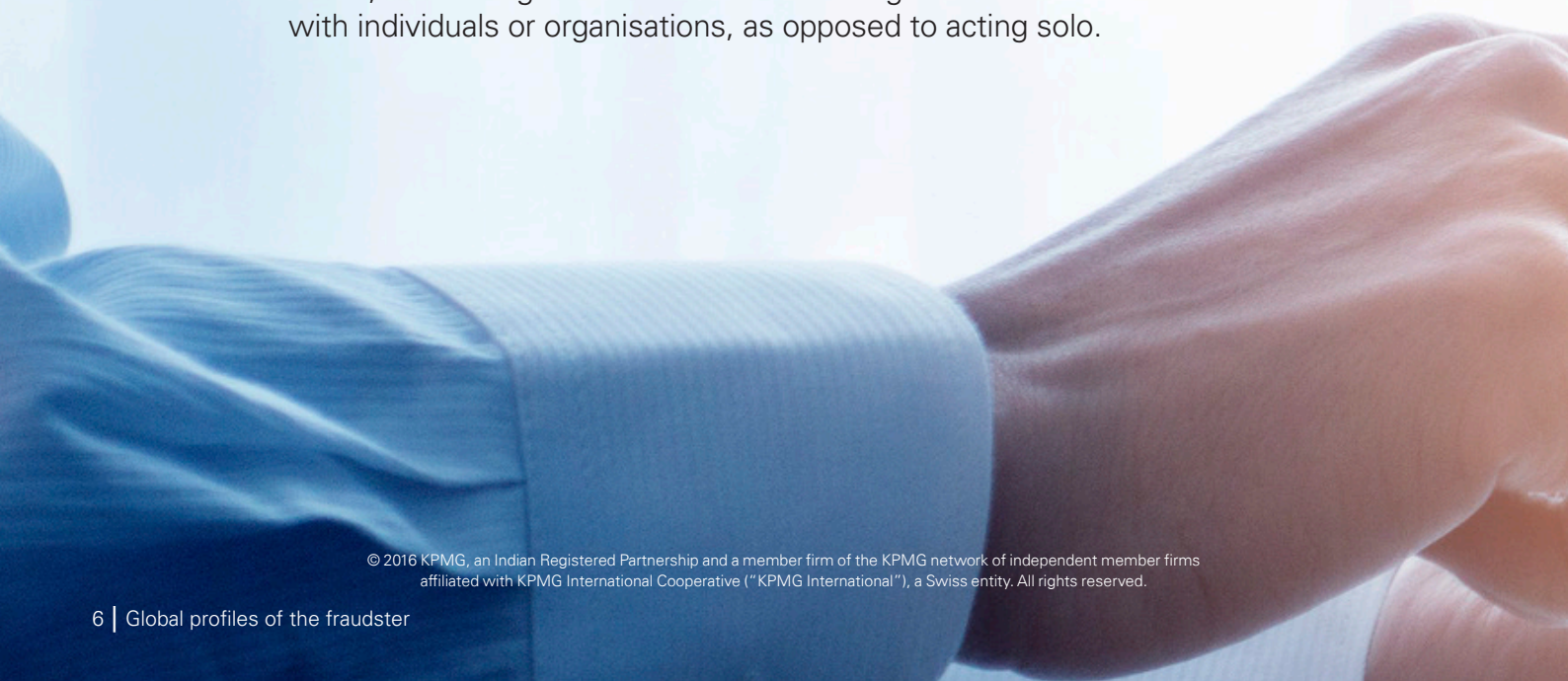
Phillip Ostwalt
Global Head of Investigations
KPMG International

Perspectives from India

Typically, a fraudster is perceived as someone who is greedy and deceitful by nature. Our global analysis has revealed that many fraudsters work within entities for a couple of years without committing any fraud, before an influencing factor – personal gain, greed, desire to look superior, or simply an opportunity to commit fraud – tips the balance.

Of the 750 fraudsters profiled for this year's survey, 56 are from India. We observed some distinctive aspects which help shape the profile of a fraudster in the Indian context. Here is what we found:

- Indian fraudsters are younger and initiate acts of fraud much earlier in their careers, compared with their global counterparts.
- The increasing incidence of technology in enabling these frauds is consistent with the trend of perpetrators being younger in our country. Most of them are at the manager and staff level.
- Fraud is more frequently perpetrated in groups, rather than alone. In fact, larger the group, bigger the damage. Additionally, weak control structures make the opportunity to commit fraud easier, reaffirming the comfort of committing frauds in collusion with individuals or organisations, as opposed to acting solo.



- Resume fraud or application fraud is a significant and growing trend observed in India, across genders. Primary areas of discrepancies include education certifications, addresses and past experience.
- Corruption may go hand in hand with fraud, exhibiting features that are different from other forms of fraudulent activity, and typically involve senior levels of management.

New fraud techniques are continually developing and organisations need to respond by updating their defenses. While technology is increasingly being used to enable frauds, little evidence indicates its use in combatting this elusive challenge.

Besides the need to stay sharp, businesses need to ensure that adequate levels of due diligence and third party intelligence are factored in, which can help organisations assess risks regularly.

We hope you enjoy reading through the report.

Mritunjay Kapur
Partner and Head
Risk Consulting
KPMG in India

Mohit Bahl
Partner and Head
Forensic Services
KPMG in India

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 seems to be growing. KPMG International's survey of 750 fraudsters worldwide found that weak internal controls were a contributing factor in no less than three quarters of them globally, and in more than half of the cases examined in India. 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 conducted by KPMG International 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. From an Indian perspective, more than half of the frauds reported were through whistle-blower hotlines, complaints and anonymous informal tip-offs.

— Globally, and in India, 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. Larger groups (say, five or more people) tend to do more harm financially than single fraudsters or small groups.

— Higher growth markets, such as India, Latin America and the Caribbean, exhibited higher collusive fraud, compared with the more developed markets like the U.S., Australia and New Zealand, where several fraudsters acted solo.

— Male fraudsters tend to collude more than women do, though the proportion of women has risen since 2010. Male fraudsters also tend to be more senior than women in the organisation.

— Groups of fraudsters very often comprise people both inside and outside the organisation. Sixty-one per cent of colluders are either non-employees, or are employees who work with people who are not. Some of them are former employees. This is a dominant trend in India, where 77 per cent of the colluder groups comprised of outsiders (20 per cent were purely external while 57 per cent were a combination of two, and only 23 per cent of colluders were purely internal).

— Technology helps both the fraudster and the organisation that is combatting fraud, and the proportion of the former was higher in India (33 per cent) compared with trends observed globally, where almost a quarter of fraudsters rely on technology. Organisations, by contrast, could do a great deal more to use technology as a tool to prevent, detect and respond to wrongdoing. At present, data analytics, as one of the key anti-fraud technologies, can sift through millions of transactions, looking for suspicious items. But only 3 per cent used proactive anti-fraud data analytics in detecting the fraudsters surveyed.

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

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

The profile of fraudster

Based on a worldwide survey by KPMG International's professionals, who investigated 750 fraudsters between March 2013 and August 2015, the typical fraudster has similar characteristics when compared to the earlier surveys conducted by KPMG International in 2013 and 2010. Across these surveys, the perpetrator of fraud tends to be male between the ages of 36 and 55 (36 to 45 in case of India), working with the victim organisation for more than six years, holding an executive position in operations, finance or general management. In India, almost an equal number of fraudsters worked with the victim organisation in excess of six years, as opposed to those in the one to four year career bracket, highlighting a distinct trend that contextualises the typical Indian fraudster.

Additional key characteristics of the fraudster revealed in the Global profiles of the fraudster 2015 survey are as follows:

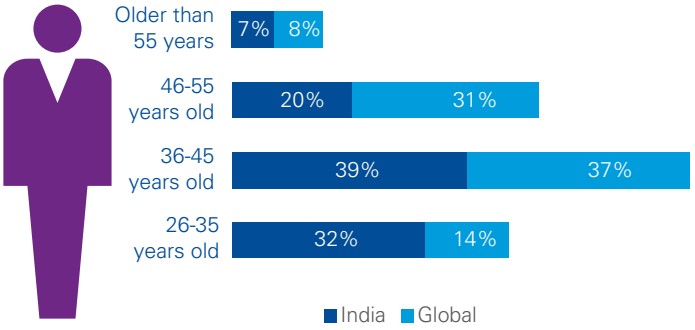
Gender and age

— Of the fraudsters surveyed globally, 79 per cent are men, although the proportion of women has risen to 17 per cent from 13 per cent in 2010. This trend is also consistent with our findings in India.

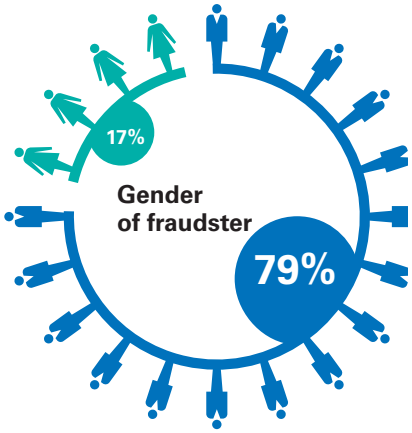
— Sixty-eight per cent of perpetrators globally, and 59 per cent of fraudsters in India (male and female) fall between the ages of 36 and 55, which is almost the same as revealed in the previous survey, published in 2013. Forty five per cent of women fraudsters, the largest cohort, fall in the 36 to 45 age group.

— In India, 32 per cent of the perpetrators are in the age group of 26 to 35 (14 per cent globally), indicating that Indian fraudsters are younger, compared with their global counterparts. This trend is also reflective in resume frauds noted in India where 61 per cent of fraudulent resumes are of people in the same age group.

Age of the Indian fraudster



*Remainder unknown age; figures above are global demographics
Source: Global profiles of the fraudster, KPMG International, 2016



*Remainder unknown gender; figures above are global demographics
Source: Global profiles of the fraudster, KPMG International, 2016

Insiders, outsiders and collusion

— Sixty-five per cent of fraudsters are employed by their respective victim organisations and a further 21 per cent are former employees. Among fraudsters who were employees, 38 per cent worked with the victim organisation for more than six years. These proportions have however remained unchanged since our survey in 2013.
Specific to India, 73 per cent of fraudsters are employed by the victim organisation.

— Globally, and in India, in case of 62 per cent of fraudsters examined, the perpetrator colluded with others.

— Global trends indicate that women are less likely to collude, with only 45 per cent of the females colluding with others compared to 66 per cent of males.

— Collusion involving more than five people increased from 9 per cent in 2010 to 20 per cent in 2015 and this trend is consistent as per the analysis carried out on the Indian cases as well.

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

Corporate title

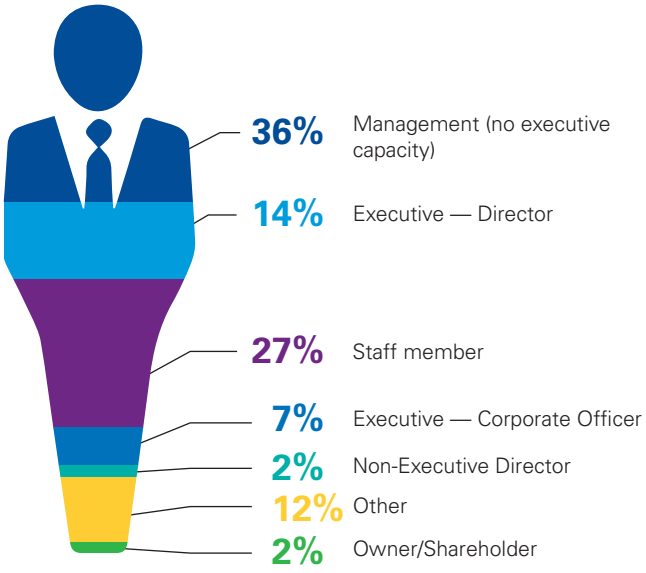
— Thirty-four per cent of fraudsters are identified as executives or non-executive directors, 32 per cent are managers and 20 per cent are staff members (In 2013, the respective ratios were 32 per cent, 25 per cent and

Years of service

Source: Global profiles of the fraudster, KPMG International, 2016

> An interesting observation in this year's survey in India finds an increasing number of fraudsters in the one to four years of service bracket (27 per cent) compared to 19 per cent globally, indicating that not only is the Indian fraudster younger, but also starts early, says Jagvinder Brar, Partner, Forensic Services, KPMG in India.

Level of seniority of the Indian fraudster



Source: Global profiles of the fraudster, KPMG International, 2016

16 per cent). In India, while 23 per cent of the fraudsters surveyed are executives or non-executives, more than half of the fraudsters (63 per cent) are at a manager and staff level, consistent with the trend of perpetrators being young in India.

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

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

Personal traits

— 38 per cent of fraudsters are perceived to be well respected, and 10 per cent are seen to be of low repute. A stark comparison was observed in case of India, as 64 per cent of fraudsters are perceived to be high performers and are well respected.

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

Circumvention of controls

— Weak internal controls are a contributing factor for 61 per cent of fraudsters globally, compared with 54 per cent in 2013. The study indicated that in Europe, 72 per cent of the fraudsters said that weak internal controls presented an opportunity for fraud. Similar was the case with 59 per cent of the respondents in North America and Oceania.

— Forty-four per cent of perpetrators have unlimited authority in their organisation and are able to override controls. Specific to India, 69 per cent of perpetrators were able to override controls within their roles. Frauds largely go undetected when anti-fraud controls are not adequate, or at times, inexistent or missing; and this problem is growing.

Characteristics of fraud

— Technology was a significant enabler for 24 per cent (33 per cent for India) of the fraudsters. For the first time, our survey includes 31 cyber fraudsters investigated by KPMG International.

— The most prevalent fraud surveyed is the misappropriation of assets (47 per cent globally and 43 per cent in case of India), which is mainly embezzlement and procurement fraud. Globally, the second most prevalent is fraudulent financial reporting (22 per cent), while in India, revenue or assets gained by fraudulent activity occupied the second position (30 per cent), with fraudulent financial reporting at third place (20 per cent).

— 24 per cent of the frauds in Africa and the Middle East are in the energy and natural resources sector and 26 percent in Oceania are in the public sector. Industrial markets, infrastructure and government and financial sectors are the highest fraud prone sectors in India.

— Sixty-six per cent of frauds were perpetrated over one to five years (72 per cent in 2013) and cost the organisations USD1 million or more; and little has changed from 2013. Trends observed in India indicate a large number of frauds perpetrated over one to two years itself (41 per cent) and are consistent with our finding of Indian fraudsters being able to perpetrate the system earlier in their careers.

— Forty-four per cent of fraudsters were detected as a result of a tip, complaint, or a formal whistle-blowing hotline, and this percentage was much higher for India, at 59 per cent. Further, 25 per cent cases in India 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 organisations face an escalating threat of cyber fraud with no let-up in the more traditional forms of wrongdoing, such as falsification of books and records. In response, many organisations 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 per cent of fraudsters (72 per cent in Europe and 54 per cent in India) in allowing the fraud to occur and go undetected.

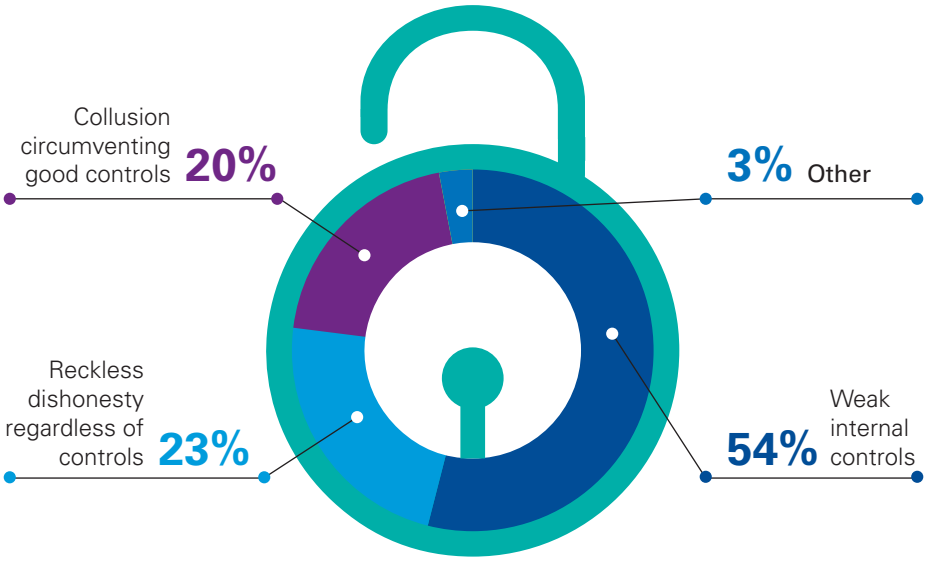
This highlights not only the scale of the management challenge for many organisations, but also the potential benefits derived from tightening anti-fraud controls, including the avoidance of financial loss and reputational costs of fraud. Simply put, fraud is less likely to occur in organisations where there are robust internal controls and monitoring.

"There is a strong correlation between internal controls and occurrence of fraud – stronger the controls, lower are the chances. Considering that weak internal controls are a significant contributing factor for 61 per cent of fraudsters, investment in stronger anti-fraud controls and a robust monitoring framework is the need of the hour." says Manoj Khanna, Partner, Forensic Services, KPMG in India.

This point is reflected in the fact that a significant number of fraudsters (14 per cent globally and in India) were detected by accident rather than by internal controls and monitoring. There are certain controls and processes that are particularly effective in combatting fraud and we endeavour to explain the same in the recommendations section. Weak controls are a significant issue for organisations victimised by fraud. Compared with the survey results in 2013, there was a big jump, (from 18 per cent to 27 per cent) 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.

> "Weak or non-existent anti-fraud controls allow frauds to occur in the first place. To make matters worse, 69 per cent of perpetrators in India were able to override controls, sometimes even through collusion. Unfortunately, organisations go about their day, losing millions to fraud, oblivious to the problems they face says Shashank Karnad, Partner, Forensic Services, KPMG in India."

Factors contributing to the facilitation of fraud in India



Source: Global profiles of the fraudster, KPMG International, 2016

What was the overriding motivation for Indian fraudsters?

Source: Global profiles of the fraudster, KPMG International, 2016

"In India, greed is the predominant motivation for 77 per cent of fraudsters compared with 66 per cent globally, says Jagvinder Brar, Partner, Forensic Services, KPMG in India. This manifests itself into personal financial gain and the desire to show better performance than what is reality. Their sense of superiority is stronger than their sense of fear or anger."

Unusual features of corruption

Fraud and corruption usually go hand-in-hand and that regulators around the world are increasingly focussing on anti-bribery and corruption controls. Of the 750 fraudsters surveyed, there were 125 perpetrators who committed 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 an organisation; 51 per cent were executives in such cases compared with 31 per cent for other types of fraud. Further, it tends to be concentrated in the office of the chief executive (26 per cent compared with 15 per cent for other types). Adding to this, Jagvinder Brar, Partner, Forensic Services, KPMG in India says, "This is an exception to the trend of younger fraudsters in India – supply side corruption tends to operate at higher levels in an organisation - in the office of the chief executive or owners in case of Indian organisations."

While 63 per cent of fraudsters engaged in corrupt practices for three years or more, 47 per cent fraudsters were involved in other frauds, but the cost of 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 kind of tip-offs, compared with 33 per cent for other types of fraud.

Organisations 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 organisations and enforcing stricter rules of business conduct, led by the U.S. 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 globally is that organisations 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 organisations are venturing into new geographical markets in search of business opportunities, including into countries where corruption is rife.

The biggest frauds override or circumvent controls

86 fraudsters were analysed, whose crimes cost organisations USD5 million or more. The frauds tended to last longer than other categories of fraud and 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 of such frauds took place across borders (34 per cent compared with 11 per cent for lesser frauds).

The fraudsters in this group are generally older than the average, with 85 per cent being male, involving executives (54 per cent versus 31 per cent 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 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 per cent) than among smaller frauds (60 per cent) and the colluders are less likely to involve external fraudsters. Almost a third (32 per cent versus 18 per cent elsewhere) involved more than five people. As one might expect, 51 per cent worked in large global firms (compared with 38 per cent for less-costly frauds).

Twenty per cent worked in financial services, versus 8 per cent for the rest of the fraudsters.

A particularly pernicious species of fraud is one conducted by groups of five or more, comprising usually males. Twenty-seven per cent of the frauds perpetrated by these large groups cost organisations USD5 million or more and continued for more than five years. "Collusion in an organisation is equivalent to cancer in a human body – prevention requires systematic controls, timely assessment for detection and a thorough investigation for clean-up response," says Suveer Khanna, Partner, Forensic Services, KPMG in India.

People can evade strong controls

Strong anti-fraud controls are important, but they are not a panacea; 21 per cent of fraudsters simply were able to disregard the organisation's controls. This trend is consistent in India, with the percentage of fraudsters going up marginally to 23 per cent. The fraudsters were seriously not concerned, despite facing the risk of getting caught. There are always likely 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. An extremely high proportion (44 per cent) of fraudsters were noted as having unlimited authority and were able to override existing controls. In India, this number shoots up to a glaring 72 per cent, a significant indicator of the lack, or in many cases, inexistent controls. "Being in a decision making position lures a person to do things that are not necessarily ethical. This is becoming more and more pervasive. It is important to understand the intent if you want to 'catch the fraudster'," says Nitish Poddar, Partner, Forensic Services, KPMG in India.

They also tend to be more damaging; 34 per cent of frauds cost organisations USD1 million or more, compared with 18 per cent of fraudsters that did not have unlimited authority.

> "**Twenty-three per cent of fraudsters in India** simply were able to disregard the organisation's controls. They were not seriously concerned about the possibility of getting caught."

Personal traits can also add fuel to the fire. According to the survey, the most frequent description of the fraudsters profiled is being autocratic and possessing a sense of superiority that is perceived to be far stronger than a sense of anger or 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 and are rarely perceived as loners. They tend to be highly respected and do not 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 shall see in the next section, fraudsters who collude are a particular threat, in part because they evade even strong controls. In organisations where anti-fraud mechanisms are tight, 16 per cent of fraudsters who collude are able to circumvent them or persuade other employees to commit fraud on their behalf.

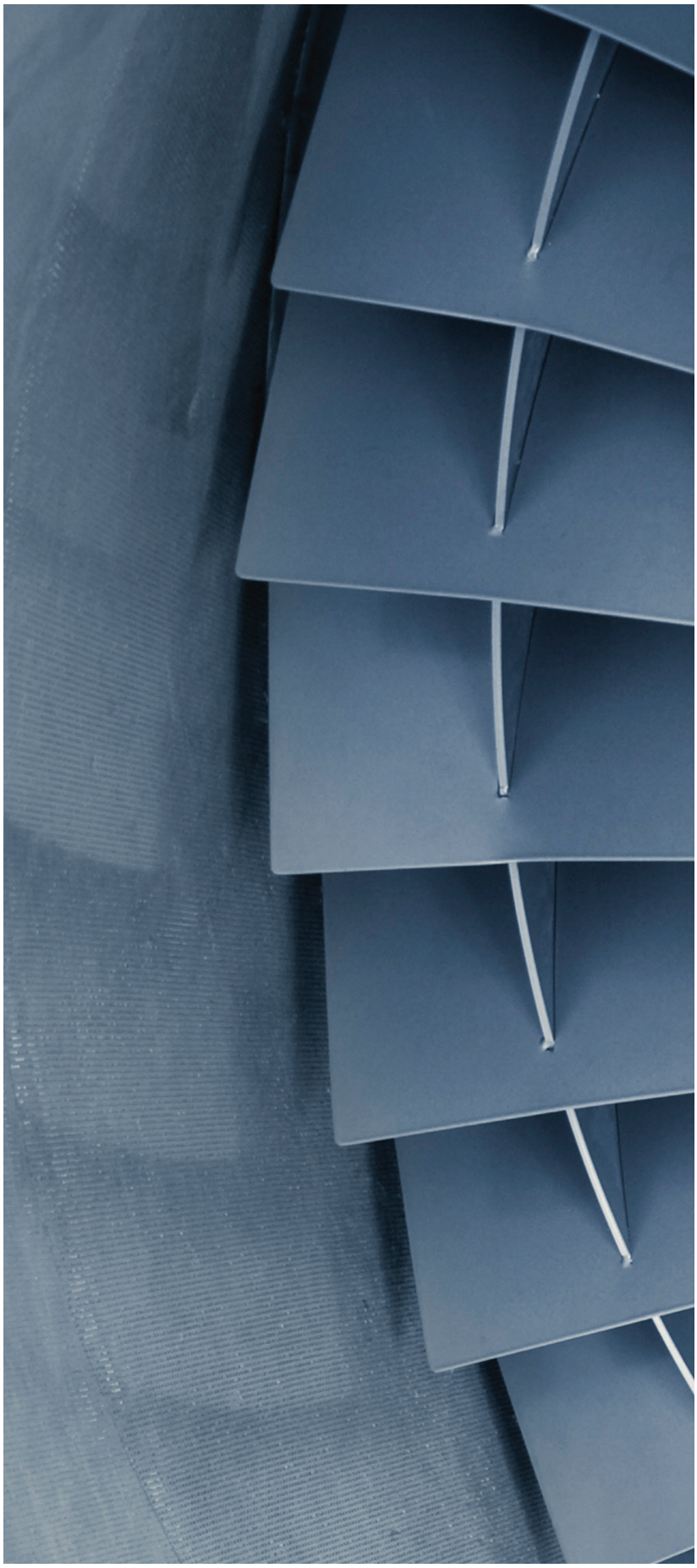
Adding to this, Shobhit Agarwal, Partner, Forensic Services, KPMG in India says, "As control structures become multi layered and it becomes increasingly difficult for individuals to beat them, there is a growing tendency towards collusion to perpetrate fraud. This is further complicated by growth in outsourcing of non-core operations by organisations."

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 armour, there has been an increase in the proportion of cases where internal controls led to the detection of fraud (from 68 per cent in 2013 to 72 per cent in 2015).

What types of mechanisms detected collusion? Of 456 such examples, 52 per cent 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 organisation 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.

"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. It also suggests that other anti-fraud procedures, such as internal audit, need to be strengthened. Organisations should ensure that different forms of control are working effectively.



Lone wolves and fraudsters who hunt in packs

For many people, corporate fraudsters conjure an image of a solitary individual who relies on his or her own ingenuity and cunningness to perpetrate the crime. However, fraudsters operating in groups are more than twice as common as those going it alone, according to the survey. In 2015, 62 per cent of fraudsters colluded with others, compared with 59 per cent in 2010. Interestingly, there are marked regional differences in the frequency of collusion. Higher growth markets, such as India, Latin America and the Caribbean, exhibited higher level of collusive fraud, compared with the more developed markets, such as the U.S, Australia and New Zealand, where several fraudsters acted solo. "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 per cent and 65 per cent respectively).

Who are the colluders? Fraudsters who collude tend to be more senior employees who have worked longer at the victim organisation than the solo fraudsters. Forty per cent were executives and non-executive directors, compared with only 28 per cent among fraudsters who acted alone. It is also striking that only 35 per cent (23 per cent in case of India) of colluders are a purely internal group. The remainder is either a non-employee of the victim organisation or an employee working with one or more outsiders.

This shows how vulnerable organisations can be to collusion.

Increasingly, these groups include outside parties. Organisations need to watch how they mitigate the rise of third parties colluding with employees regularly, says Mohit Bahl, Partner and Head, Forensic Services, KPMG in India.

Colluders tend to do a lot more damage than individual fraudsters. Mohit further adds, "Larger the group, bigger the damage." Thirty-four per cent of collusive fraudsters cost their organisations USD1 million or more, compared with16 per cent of soloists. Colluders tend to perpetrate larger frauds and escape detection for longer.

"A strong third party risk management programme which ensures that comprehensive due diligence is carried out on vendors, channel partners and suppliers, is a sound way of combating fraud and assessing risks regularly," says Maneesha Garg, Partner, Forensic Services, KPMG in India

"Increasingly, these groups include outside parties. Organisations need to watch how they mitigate the rise of third parties colluding with employees regularly, says Mohit Bahl, Partner and Head, Forensic Services, KPMG in India."

Moreover, the pattern of detection is quite different. Solo fraudsters are mostly caught as a result of management reviews, by accident or via internal audit. For colluders, the main methods of detection are through whistle-blowers, management reviews 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. Moreover, the pattern of detection is quite different. Solo fraudsters are mostly caught as a result of management reviews, by accident or via internal audit. For colluders, the main methods of detection are through whistle-blowers, management reviews 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.

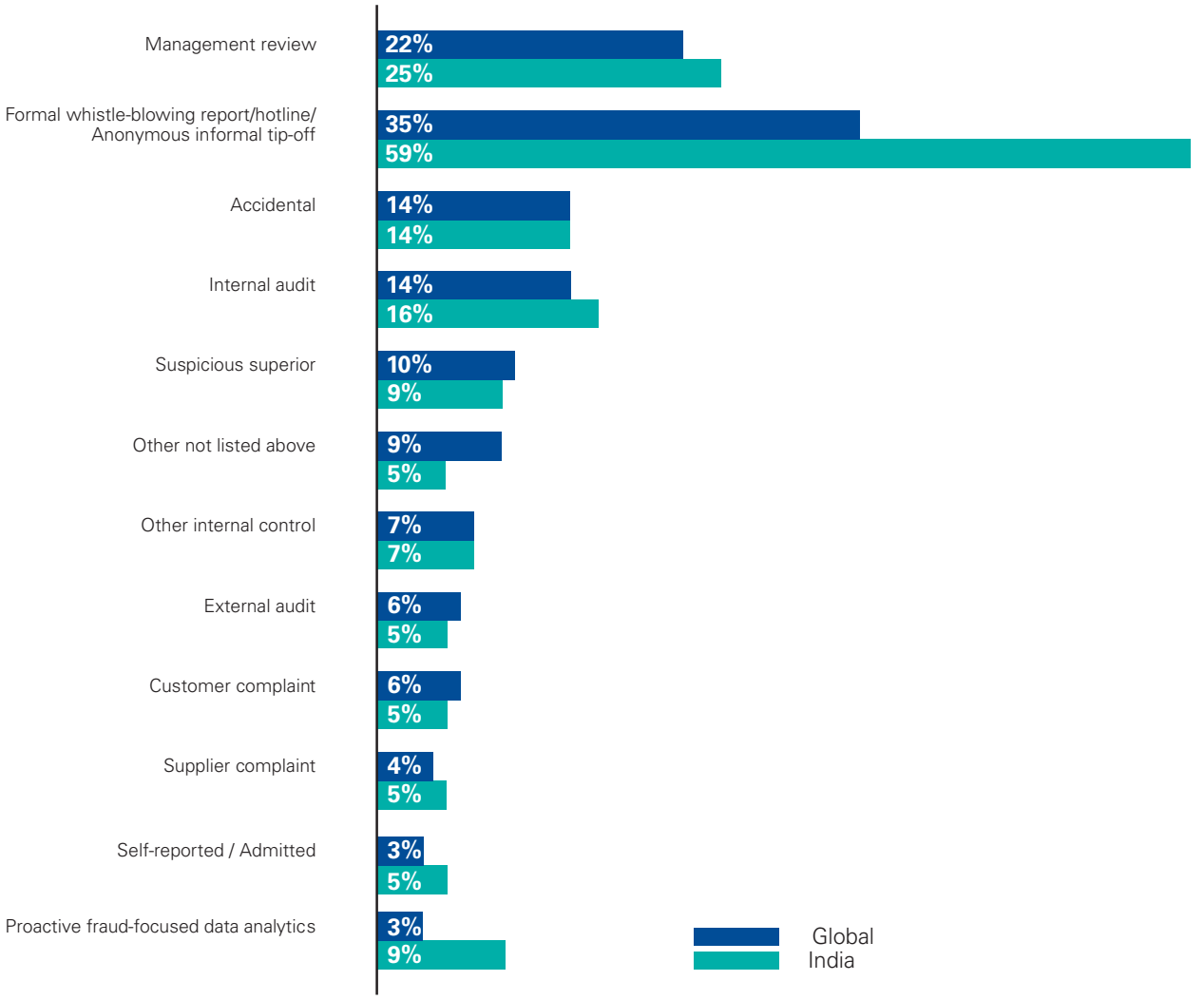
Fraudsters acting alone tend to be more junior than their collusive counterparts. Weak internal controls are a bigger factor for solo fraudsters than colluders (66 per cent versus 58 per cent). As a result, more are caught by accident than colluders (19 per cent versus 10 per cent).

When it comes to comparing the genders, 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 per cent against 45 per cent respectively). Women are, however, colluding more than they used to. The proportion of groups that include both genders rose from 34 per cent in 2010 to 47 per cent in 2015.

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

But over time, the differences in fraudulent activity between genders have narrowed somewhat, as women have risen through the ranks. Female fraudsters were more frequently in management in 2015 compared with 2010 (38 per cent versus 28 per cent) and the tendency for women to collude has gone up.

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, both at global and Indian levels. The same is true when comparing collusive fraudsters who are inside the organisation and those who are outside it. Here, the picture is more complex because there are three groups to analyse, purely internal (35 per cent), purely external (18 per cent) and a combination of the two (43 per cent). "Organisations have to design anti-fraud mechanisms that look both ways, inside and outside. They also need to be aware of the possibility that a lone, fraudster on the inside may be working with a sizeable group of people on the outside. There are many permutations organisations 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. Around forty-two per cent of frauds perpetrated by internal fraudsters resulted in the loss of USD1 million or more, compared with 32 per cent and 25 per cent, 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 per cent compared with 16 per cent), apart from having 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 per cent versus 37 per cent, respectively).

Maneesha Garg, Partner, Forensic Services, KPMG in India says, "Sound screening processes for both employees and third parties allow organisations to protect the susceptibility of fraud perpetration. With the fraudster in India being younger and this group accounting for majority of hiring desires of organisations, the need for robust gate keeping cannot be over emphasized. Verifications is no longer just a check in the box, but a mandate."

The surprising revelation of resume fraud

Resume fraud is a significant trend observed in India. Thirteen per cent of resumes screened by KPMG in India's Verifications practice indicated discrepancies. Further, the fraud has also seen a 14 per cent increase since 2013.

Primary areas of fudging included education certifications, addresses and past experience.

Maximum instances of resume fraud is observed in the age group of 25 to 35 years at 61per cent.

Further, this trend is observed to be common amongst both genders, with females fast catching up to their male counterparts. However, in the age group of 36 to 45, the gender fraud ratio reverses where males account for twice the number of resume frauds.

Percentage of frauds resulting in a loss of USD1 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

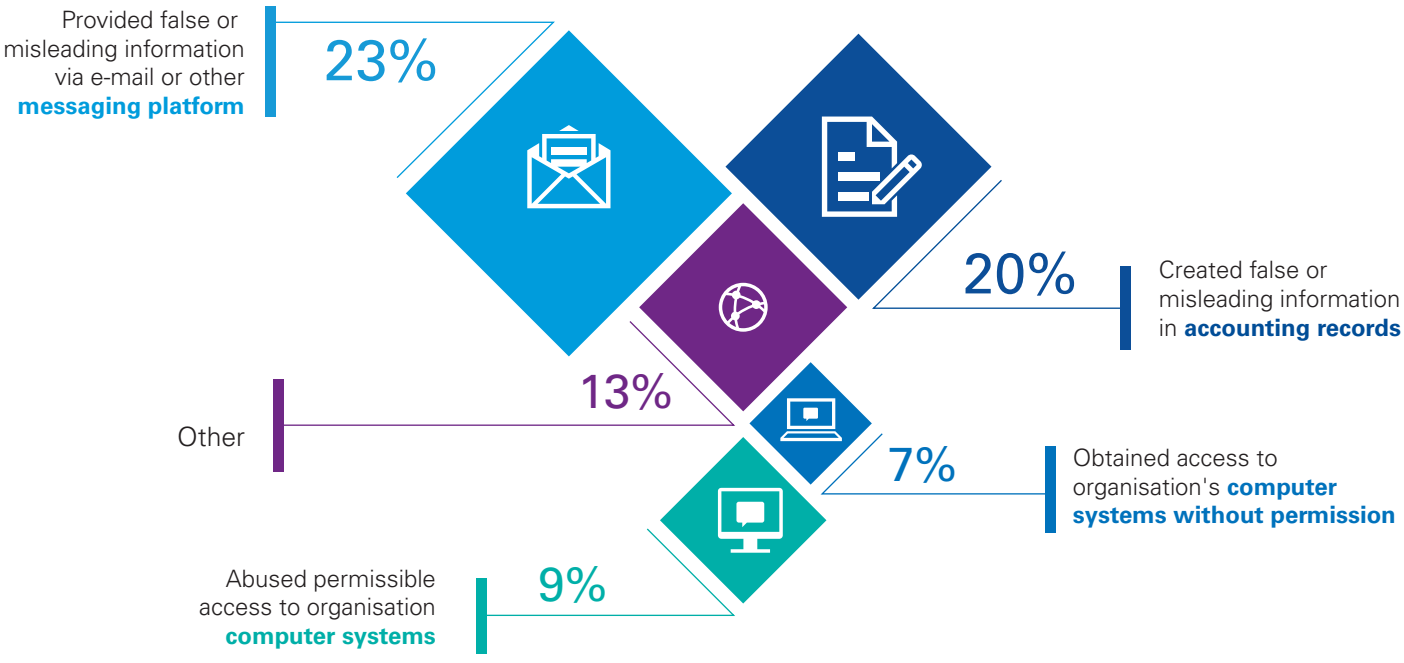
> Organisations have to design anti-fraud mechanisms that look both ways, inside and outside. And they need to be aware of the possibility that a lone, fraudster from the inside may be working with a sizeable group of people on the outside. There are many permutations organisations must guard against.

Technology helps and hinders fraudsters

Technology is a double-edged sword. Technological advances provide more powerful tools in strengthening an organisation's defenses against fraud, as well as a means for fraudsters to find areas of vulnerability to penetrate. However, our survey suggests that technology is more frequently used in perpetrating fraud than in detecting it. Technology was a major enabler for 24 per cent of fraudsters globally and this trend was significantly higher in India at 33 per cent.

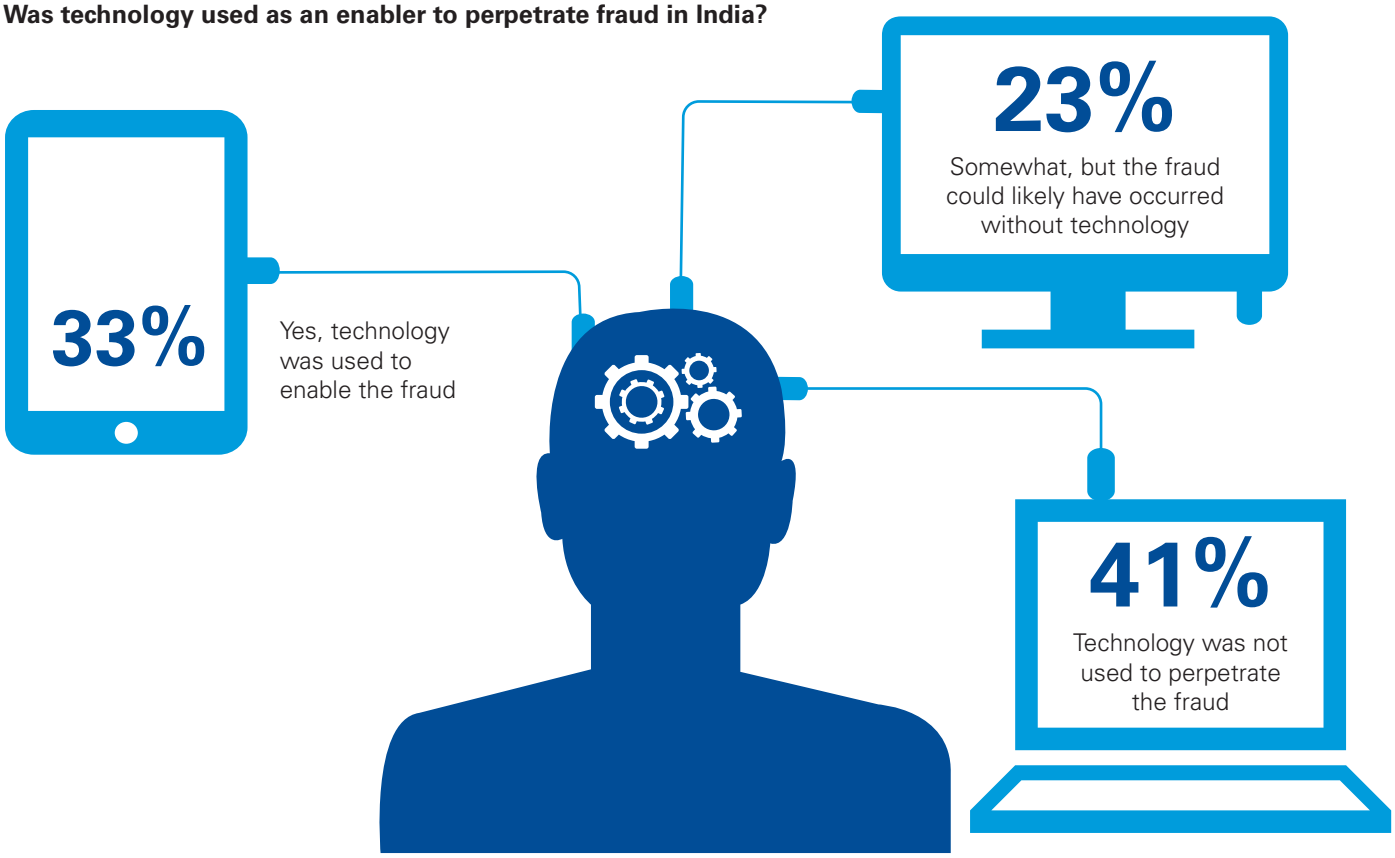
Examples of technology-enabled fraud include: gaining unauthorised electronic access to confidential information, and posting an accounting journal entry to camouflage a misappropriation. Somewhat surprisingly, the proportion of technology-enabled frauds was lowest in the regions of Europe (18 per cent)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

How technology was used to perpetuate fraud in India



Source: Global profiles of the fraudster, KPMG International, 2016

Was technology used as an enabler to perpetrate fraud in India?



Source: Global profiles of the fraudster, KPMG International, 2016

Given the size of organisations and their geographical diversity, data analytics can act as an important tool to combat fraud. An increasing number of organisations are introducing data analytic solutions to search for unusual transactions amidst millions of day-to-day sales and purchases, but it does not appear to be fully deployed by organisations. Proactive data analytics, searching for fraud amid anomalies and suspicious business activity account for only 3 per cent of frauds detected.

In technology-enabled frauds, the fraudster tends to be younger (60 per cent are aged between 26 and 45 years old. In India, this number has risen to 71 per cent, consistent with the trend of the Indian fraudster being young in India, when compared globally). "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 U.S. Some 24 per cent of technology-enabled frauds were caught accidentally, the most frequent form of detection, compared with 11 per cent for frauds that are not enabled by technology. This provides further evidence that organisations could employ technology more forcefully to combat technology-dependent fraud. In some ways, accidental detection is a sobering reminder that controls are ineffective.

"Technology is a huge medium for the 'modern day fraudster'. Interestingly, organisations are not yet focussing and investing in predictive forensic mechanisms. Advanced analytics can assist organisations in staying ahead of fraudsters," says Ritesh Tiwari, Partner, Forensic Services, KPMG in India.

> Technology is a double-edged sword. Technological advances provide 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

Cyber fraud, is one of the most frequently cited threats by KPMG professionals around the world. Many have noted that organisations are aware of the threat but do not think they will be targeted. Therefore, may not know that they have been attacked, signifying a lack of preparedness against the threat. "We find that executives know that hackers and criminal organisations can wreak havoc on organisations; they read about such cases almost every day in the media. But they often do not 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 U.S.

The survey samples included 31 recent perpetrators of cyber fraud that have been investigated by the firm, but this may just 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 organisation, often working with outside syndicates. Nine were associated with organised criminal groups and seven were individual criminals, hacking from outside.

The survey reveals that one of the main objectives of cyber fraud is the theft of personal data and intellectual property, senior executives' e-mails, strategic access to organisation data, and denial of services. The Federal Bureau of Investigation of the U.S. says[1] that there has been a sharp increase in 'business e-mail crime', with more than 12,000 victims being affected globally.

Fraud occurs when a criminal sends an e-mail purporting to be from a senior executive and directs an employee to wire money to an overseas bank account. The FBI has stated that it cost businesses about USD1.2 billion in 2013-2015.

"Cyber threat from insiders and outsiders is a growing challenge faced by all organisations. The perpetrators on the inside know the systems and process weaknesses which help facilitate fraud. Cyber criminals are no longer novices. There are international cyber-crime syndicates with a network of hackers who are able to carry out well planned attacks. Organisations need to carry out cyber risk assessments along with simulated cyber-attack drills and develop a robust incident response mechanism," says Sandeep Gupta, Partner, Forensic Services, KPMG in India.

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

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

How to combat fraud

This report is based on the survey results analysed by KPMG International's professionals. The question for organisations is how should they combat fraudsters? Based on the analysis of the data, four main recommendations emerge:

Fight back with technology — The survey reveals that a significant number of fraudsters use technology to perpetuate a fraud (a trend observed in India in over a third of the fraudsters analysed). However, we could find little evidence that organisations are using technology to combat fraud.

Organisations are often eager to reap the potential benefits of data analytics and its ability to sift through huge amounts of information they accumulate. However, they often buy off-the-shelf solutions that do not integrate well and are eventually scrapped. It is far better to look for a more extensive approach that can cover most of an organisation's important surveillance and detection needs. They may even have the software tools 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 monitor continuously by means of automated computer programmes, 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 organisations 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 organisation's legal environment and business operations. It is a wise, initial step, to stress-test the organisation's environment (in terms of activity-based controls and entity-level controls), especially when organisations engage a group of professionals that are well

> "Organisations today must adopt anti-fraud analytic solutions and leverage technology to combat fraud. The use of threat-monitoring systems and data analytics is increasing and can highlight anomalous or suspicious behaviour by monitoring personal behavior, analysing computer usage, public records and social media."

Recommendations:

Source: Global profiles of the fraudster, KPMG International, 2016

versed with changing risks, operations, compliance, and legal situations.

Cyber security assessments may, if the organisation 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 organisations facing similar threats, usually in the same industry.

Know your business partners and third parties — Organisations should not only look inward when it comes to fraud, they should also closely monitor their business partners and other third parties that are conducting business on their behalf. As organisations extend their reach across the globe, they become 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 one of the leading business practices, and a core element of active leading compliance programmes.

Furthermore, organisations should, from time to time, ensure that their suppliers are billing them as per their contractual agreement and they should use their right to audit clause which is normally included in such agreements. Technology has enabled organisations 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 senior managers, who have been with the organisation 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 as. Fraudsters can slip up. If things do not 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 organisation's reporting mechanisms, such as a hotline. Nurture a climate of trust in which staff members do not fear for their jobs if they raise a red flag. Once an alarm is sounded, take appropriate action to inquire or investigate the activity.

These steps may 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 is vigilant and business is carried out with integrity, fraud is likely to subside. It is an objective worth aiming for.

Methodology

The survey is based on a questionnaire prepared by KPMG's 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 organisation 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 investigated involved more than one fraudster). In 2013, the total was 596 fraudsters and in 2010 it was 348 fraudsters. The frauds in the 2015 survey occurred in 81 countries (including Hong Kong and Puerto Rico).

***percentages may differ by one per cent due to rounding**

Acknowledgements

Aashruti Kak
Déan Friedman
Daniel Viray
Estelle Wickham
Iqra Bhat
Jack Martin
Jagvinder Brar
Jimmy Helm
Kajen Subramoney
Kemi Okhumale
Krishna Pandala
Laura Dobrotka
Maneesha Garg
Manoj Khanna
Matt Hansen
Matt Dixon
Masako Asaka
Mohit Bahl
Muhammad Hoosain
Nick D'Ambrosio
Nitish Poddar
Priyanka Agarwal
Rahil Uppal
Renee Gooden
Ritesh Tiwari
Sandeep Gupta
Sandra Cusato
Shashank Karnad
Shelley Hayes
Shobhit Agarwal
Stephan Drolet
Suangna Singh
Suveer Khanna
Tom Keegan
Tracey Walker
Victoria Malloy

Contact us

Nitin Atroley
Partner and Head
Sales and Markets
T: +91 124 307 4887
E: nitinatroley@kpmg.com

Mritunjay Kapur
Partner and Head
Risk Consulting
T: +91 124 307 4797
E: mritunjay@kpmg.com

Mohit Bahl
Partner and Head
Forensic Services
T: +91 124 307 4703
E: mbahl@kpmg.com

kpmg.com/socialmedia

kpmg.com/app

Available on the App Store