KPMG

FORENSIC

Profile of a Fraudster Survey 2007

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

Content

1 Introduction

Who commits fraud?

At first glance, an average fraudster[1] is not much different from an average person. Consequently, it is often extremely difficult to detect fraudulent acts. But upon reflection, the following circumstance must be considered: Why are people often caught unaware when somebody is accused of fraud? Because it is usually the colleague who is known to be helpful, polite and inconspicuous. But most importantly it is the colleague that enjoys the absolute trust of both superiors and colleagues.

This fact highlights the importance of recognizing trust as a main risk factor, making it all the more crucial for management to exercise a well-considered balance between trust and control.

This insight does not answer the original question and should not lead to the assumption that each trusted employee is a potential fraudster; rather it leads to the question:

Why do people commit fraud?

From a theoretical point of view there are three important factors concerned with committing fraud: opportunity, motive, and rationalization, also known as the fraud triangle.

Opportunity generally occurs through weaknesses in the internal controls and creates an atmosphere where fraudsters believe they are likely to be successful and undetected. Therefore companies primarily focus their prevention efforts on this aspect of the fraud triangle by enforcing certain types of controls and by implementing effective fraud risk management policies. Trust, however, though important in business often becomes the door opener for fraudsters.

Motive often develops from financial pressure resulting from a fraudster's excessive life style, or from the gap between the financial remuneration earned and the responsibility held by the individual, or pressure to meet financial targets, or the superiority complexes of the individual or basic greed.

Rationalization is the fraudster's internal dialogue that provides the self justification for his actions. The fraudster convinces himself/herself that he/she is owed this remuneration by the employer.

1 The term "fraudster" in this survey is used as an non-technical term, not limited to those perpetrators who committed fraud in a legal sense, but to white-collar crime in general.

Insight, awareness & recognition – Turn expertise into added value

Becoming aware of the above mentioned facts, gaining insight into the motivations of a fraudster and recognizing the enormous threat every company is exposed to are the first important steps in establishing and implementing an effective and sustainable fraud risk management system.

The aim of this survey is to combine theory with practicality. KPMG's Forensic professionals offer extensive knowledge and experience gained over decades, in organizations of all sizes, in various branches, in diverse geographical regions and encountering all types of fraudsters.

Profile of a Fraudster Survey

By basing the KPMG's Profile of a Fraudster Survey 2007 on hundreds of actual fraud investigations conducted by KPMG Forensic departments within the EMA region (Europe, Middle East and Africa), the results reveal a comprehensive profile of those who commit fraud, the conditions in which fraud takes place and the resulting actions. This survey is not strictly representative in the statistical-mathematical sense because it solely covers the reported profiles and only those investigated by KPMG. Despite this fact it is unique for two reasons. First, it is significant that this survey focuses on the perpetrator. Second, it is extraordinary because it is based on actual fraud investigations and not on voluntary self declarations of interviewed organizations. The result is an overall profile of the perpetrator within the context of the environment in which he operated and the circumstances in which he was located and acted.

The results paint an interesting and instructive picture of "the typical fraudster." In eighty-nine percent of the profiles, the fraudsters committed fraudulent acts against their own employers. In twenty percent of these profiles, an external perpetrator was involved. Interestingly, the tenure of employment does not have a positive influence – rather the contrary: more than fifty percent of offenders have been with their company for more than six years. In sixty-eight percent of profiles fraudsters acted independently. In only five percent of profiles more than five people were involved. In ninety-one percent of profiles perpetrators were not content with one fraudulent act, but acted multiple times – often over a period of several years.

Lone operators represent the greatest white collar crime risk for companies. The survey results indicate that two thirds of all primary internal perpetrators are members of the top management. This finding highlights a significant risk, based on the concept of trust, as company executives are privy to highly confidential information and have the potential to cause the most harm to the organization.

The findings reinforce the notion that the overriding motivations for white-collar crime are greed, opportunity and the pressure to meet budgets and targets. The last two reasons particularly should ring a warning bell and raise the awareness of employers, because they provide at least one aspect of the fraud triangle and offer a reason for a second one.

Pablo Bernad Ramoneda
Partner, Regional Chairman Forensic Europe, Middle East and Africa (EMA)

2 Methodology

Approach

Information concerning details of fraud investigations conducted by forensic departments of KPMG in Europe, India and the Middle East and South Africa (EMA) over the past few years was gathered through an online questionnaire. The survey reveals the following information:

- fraudster profile including personal details and information regarding the fraudulent acts.
- conditions for enabling the fraudulent acts and the surrounding factors.
- follow-up actions by fraud victims.

General Conditions

Out of several hundred fraud investigations conducted by Forensic EMA in the last few years only profiles of white collar crimes and profiles with clearly identifiable fraudsters were included in the survey.

Excluded were those fraudulent acts considered to be of no material value, profiles of misconduct or where the suspected fraud could not be substantiated in the course of the investigation and profiles where a certain amount of requested details could not be provided.

360 profiles were selected for analysis.

All mentioned figures are percentages and all amounts refer to the currency Euro (EUR).

3 Executive Summary

Fraudster facts and figures

Personal details

- 70 percent of fraudsters were between the ages of 36 and 55 years old.
- 85 percent of perpetrators were male.
- In 68 percent of profiles the perpetrator acted independently.
- In 89 percent of profiles the fraudsters were employees committing fraudulent acts against their own employer, whereas 20 percent involved complicity with an external perpetrator, resulting in the conclusion that in only 11 percent of all profiles the companies were attacked purely by externals.
- Members of senior management (including board members) represent 60 percent of all fraudsters. An additional 26 percent of profiles involve management level persons bringing the total to 86 percent of profiles involving management. This result highlights a risk that every company faces: executives are entrusted with sensitive company information and yet are also often in a position to override internal controls.
- In 36 percent of profiles the perpetrator worked for their company for 2-5 years before committing fraud. In 22 percent of profiles the fraudulent employees registered more than 10 years of service at the victim's organization. In just 13 percent of profiles the fraudster was with the company for less than 2 years prior to committing fraudulent acts.
- The internal fraudster most often works in the finance department followed by operations/sales or as the CEO.

Fraud details

- Misappropriation of money was revealed as the most common type of fraud.
- In 83 percent of profiles the fraudsters acted nationally and not internationally.
- 91 percent of perpetrators did not stop at one single fraudulent transaction but rather performed multiple fraudulent transactions; every third perpetrator acted more than 50 times.
- A total loss of 1 million EUR and more per fraudster and profile was caused by every second fraudster in Europe, by almost every third perpetrator in South Africa and by every fourth offender in India and the Middle East.
- In 24 percent of profiles the timeframe for perpetrating fraudulent acts was less than 1 year. In 67 percent of profiles fraudsters acted within a timeframe between 1 year and 5 years until they were exposed or stopped their fraudulent activities. This result generates questions concerning the effectiveness and the quality of existing internal controls: why were they not able to discover or stop fraudulent acts within the recurring standard controls in more than two thirds of all profiles?

Psychological & additional circumstances

- Greed and opportunity (when taken together account for 73 percent of profiles) are indicated to be the overriding motivations for fraud.
- No prior suspicion existed in more than half of the profiles, but in 21 percent of profiles the companies did not act, even though there was prior suspicion. This raises many questions. Such as, are we, as a society too trusting and unwilling to investigate unless the facts are overwhelming?
- Perpetrators were able to commit fraud by primarily exploiting weak internal controls, in 49 percent of profiles.
- Fraudsters were mainly detected by whistle blowers or management reviews (accumulated 46 percent).

Fraud management within the concerned organization

- In 50 percent of profiles companies did not communicate the details of the fraud within the organization. In 15 percent of profiles companies revealed information concerning the fraudulent acts only selectively.
- Besides the external investigation conducted by KPMG the companies mainly carried out internal investigations, took disciplinary or legal actions and/or involved the police. Only in 2 percent of all profiles, the companies took no additional action or sanction.

Company facts & figures

- All sectors are almost equally affected by white-collar crime, except for the chemicals, pharmaceuticals & biotech sector, which appear to be less impaired.
- In Europe in half of the profiles the turnover of the companies that suffered damage, was less than 50 million EUR. While in South Africa it was 63 percent. In India and the Middle East the companies with a turnover of less than 50 million EUR and between 50 and 500 million accounted for 34 percent each.

Mitigating factors

Just as the fraud triangle tries to explain the causes of fraud using three headings we also see the mitigating factors in the three areas: prevention, detection and response.

Prevention

- *A comprehensive fraud and misconduct risk assessment* helps management understand their business unique risks, identify gaps or weaknesses in their controls and develop a plan for targeting the right resources and controls.
- *A well-implemented code of conduct* is one of the most important mechanisms to communicate with employees about acceptable business standards and to raise awareness of management's commitment to integrity.
- *An appropriate employee and third party due diligence* is an important part of an effective fraud and misconduct prevention strategy, especially for positions with authority over the financial-reporting process.
- *A carefully planned communications and training program* will raise employee awareness of their obligations concerning fraud and misconduct controls.

Detection

- *Hotlines* provide employees and third-parties with a way to report possible fraud and misconduct and to seek advice when the appropriate course of action is unclear.
- *Auditing and monitoring plans* based on the organization's fraud risk assessment process gives higher risk issues priority and facilitates fraud and misconduct detection more effectively.
- *Proactive forensic data analysis* tools – such as sophisticated analytic testing, computer-based cross matching, and non-obvious relationship identification – can help identify potential fraud and misconduct that otherwise would remain unnoticed by management, possibly for years.

Response

- *A thorough and well-planned internal investigation* should be conducted when information relating to actual or potential fraud or misconduct is uncovered.
- *A disciplinary system* detailing enforcement and accountability protocols is key to effectively deterring fraud and misconduct and signaling that managing fraud and misconduct risk is considered a top priority.
- *Public disclosure of fraud and misconduct* should be considered for combatting or preempting negative publicity, demonstrating good faith and assisting in putting the matter to rest.
- *Remedial actions should be taken* once fraud or misconduct has been discovered, e.g.
  - voluntarily disclose the results of the investigation to a regulator or other relevant body
  - remedy the harm caused
  - examine the causes to help ensure that risk is mitigated
  - discipline those involved as well as those in management positions who failed to prevent or detect such events
  - communicate to employees that management took appropriate, responsive action.

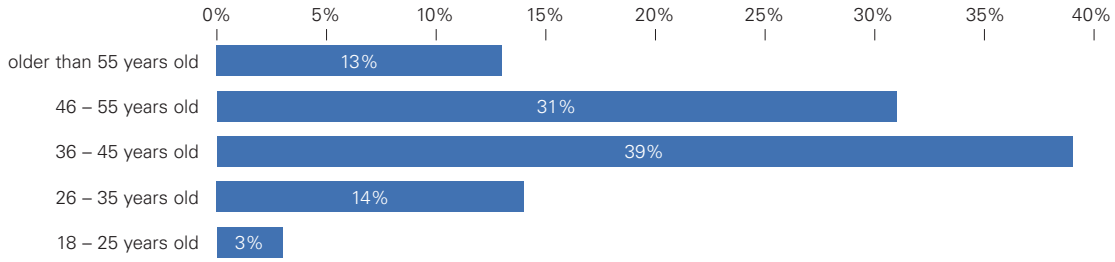
These mitigating factors are extensively covered in KPMG Fraud Risk Management White Paper, Developing a Strategy for Prevention released on 6 November, 2006.

4 Fraudster Facts & Figures

This survey provides a comprehensive overview of a fraudster's profile – including personal traits, fraudulent act details, conditions surrounding the fraud, company decisions for dealing with fraudulent acts, and affected company background information.

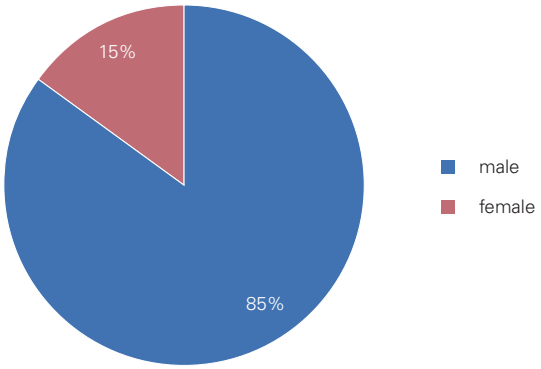
4.1 Personal Details

Age of fraudster



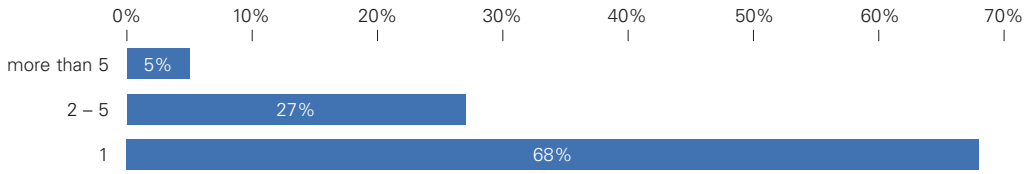
In 70 percent of profiles the perpetrators were between the ages of 36 and 55 years old. Frequency of fraudulent acts committed by people between the ages of 26 and 35 is similar to those acts committed by people over 55 years old.

Gender of fraudster



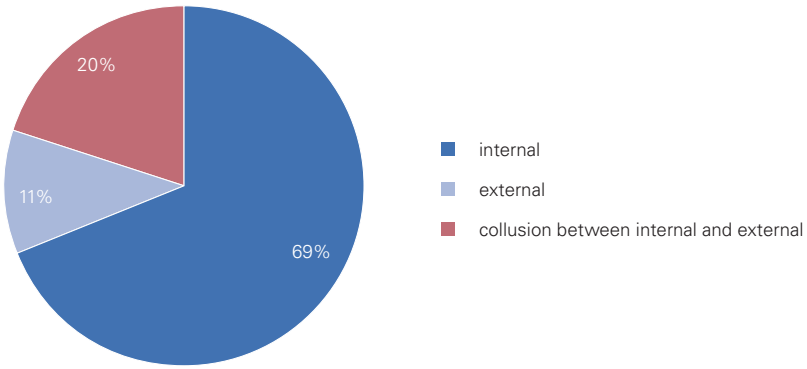
In 85 percent of profiles fraudsters were male. However, female perpetrators are not to be ignored. This statistic could be influenced by women's under-representation in management positions and therefore more limited access to sensitive information than their male colleagues. Significantly, women participated as a conspirator in every fourth profile where a conspirator was involved.

Number of fraudsters



In 68 percent of profiles the perpetrator acted independently. In 27 percent of profiles, perpetrators acted in groups of two to five conspirators. A group of more than five perpetrators only acted in 5 percent of all profiles.

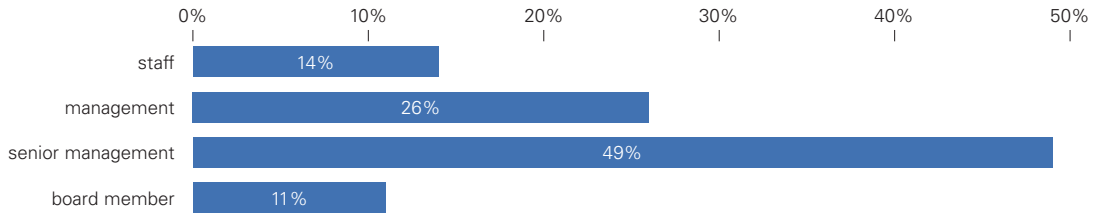
Fraudster's relationship to the organization that suffered damages



In 89 percent of profiles the company concerned was damaged by its own employees. In 20 percent of these profiles the employee acted together with an external perpetrator. Only in 11 percent of profiles were external individuals solely responsible for fraudulent acts. Results reveal that employees represent the greatest risk for the perpetration of white collar crime.

In the following sections a closer look is taken at these two groups and detailed information is provided on employees that damaged their own employers ("internal fraudster") as well as those that caused damage to a company as "external fraudsters."

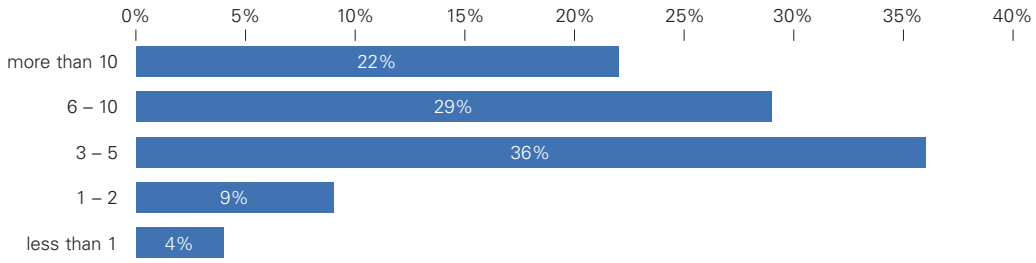
Internal fraudster – seniority



According to this survey 86 percent of fraudsters held management positions and 60 percent of these persons belonged to senior management and/or board of directors. The inherent responsibilities, trust associated with these positions, ability to override internal controls, internal knowledge and access to confidential

company information that come with a management position are essential for a company's success, but also create a risk that fraudulent acts may occur.

Internal fraudster – years of service at the victim's organization

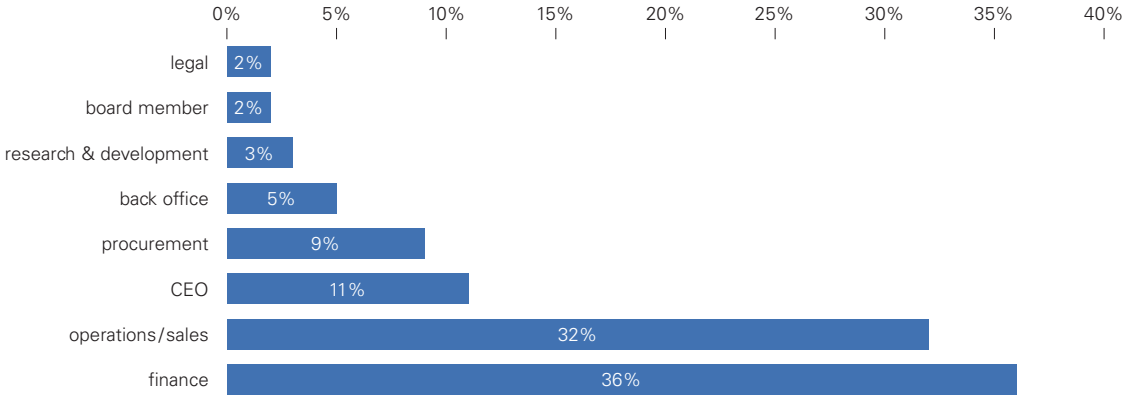


Employee tenure, is it a mitigating or contributing factor affecting the probability of fraudulent acts occurring?

Only 13 percent of the internal perpetrators involved with this survey commit fraud within the first two years of working with their company – and only 4 percent acted within their first year of employment. Most fraudulent acts are committed by employees who have been working with a company for more than two years. In 36 percent of profiles they stayed with the company between 3 to 5 years and in an additional 29 percent of profiles they were employed between 6 and 10 years. Results reveal that the tenure of employment does not seem to influence an employee's loyalty. In 22 percent of profiles employees committed fraud against their company even after 10 years and more of employment.

These results also raise the question of whether or not some new employees join an organization with the intent to commit fraud or if they only develop the "criminal inclination" once they have gained the trust of their colleagues and superiors and have identified weaknesses in internal controls and opportunities for fraud within the company.

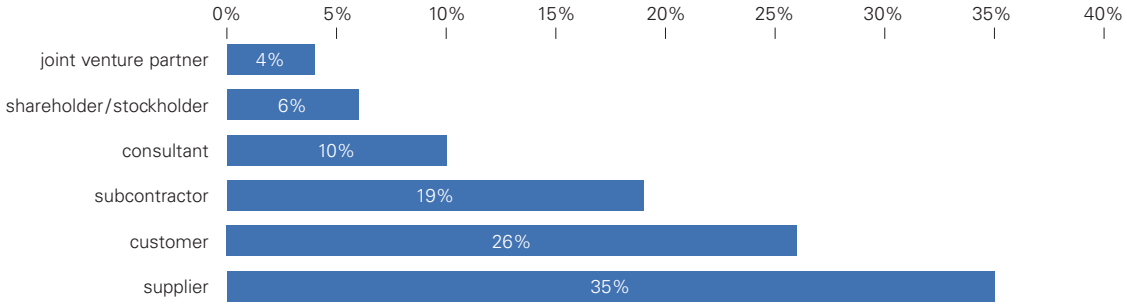
Internal fraudster – department / function



Perpetrators most commonly worked in the finance (36 percent) or operations/ sales (32 percent) departments or, as CEO (11 percent). Notably also members of the board are reported to belong to the group of fraudsters, but only in a small number of profiles. Nearly all other areas are also affected but play a less important role.

The access to and responsibilities for accounts, cash, checks, financial reports and credit lines offer a significantly higher opportunity for committing and concealing fraudulent acts than for employees working in other departments. In the finance department, two thirds of fraudulent acts occur within the controlling departments and one third of fraudulent acts occur in accounting. Although procurement and production departments are also said to be vulnerable, these departments were involved in less than 10 percent of profiles in this survey.

External fraudster – relationship to victim's organization



With regards to the relationships external perpetrators have towards the organization they damaged, the results show that nearly all possibilities are represented – although they are mainly suppliers, customers and subcontractors. As invoices and credit lines are involved in the relationships between a company and their suppliers and customers, there is an increased opportunity for fraud to occur.

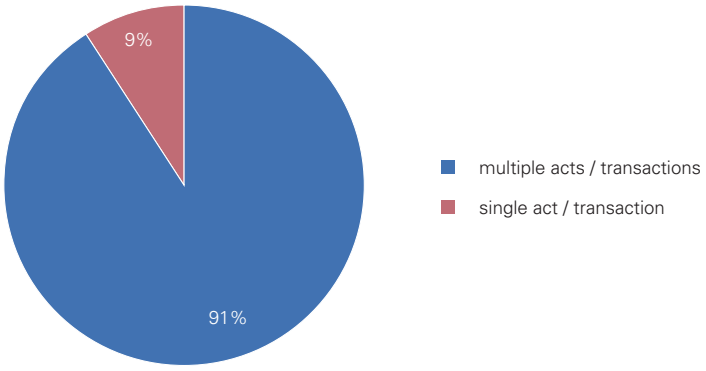
Analysis of the conspirators was also conducted in the same manner as the primary perpetrators. The results indicate that accomplices' motivations and profiles are almost identical to the primary perpetrators.

4.2 Fraud Details

In the following section the survey focuses on another facet of a fraudster's profile: the offence committed by him. How did he proceed? What was the damage he/she caused?

Number of fraudulent acts/transactions per fraudster and profile
The following two charts provide information about the number of times the perpetrators acted – was it more common to commit one act or to separate their acts into a multitude of fraudulent transactions?

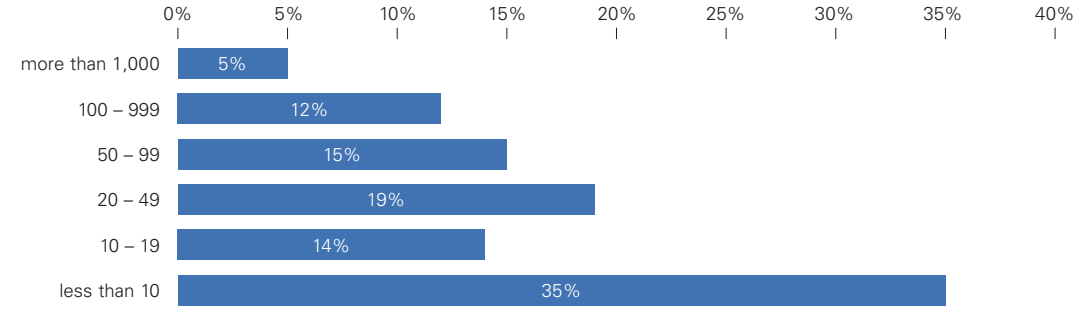
Single or multiple acts/transactions



In 91 percent of profiles the perpetrators did not leave it at one single fraudulent act, but committed repeated acts of fraud.

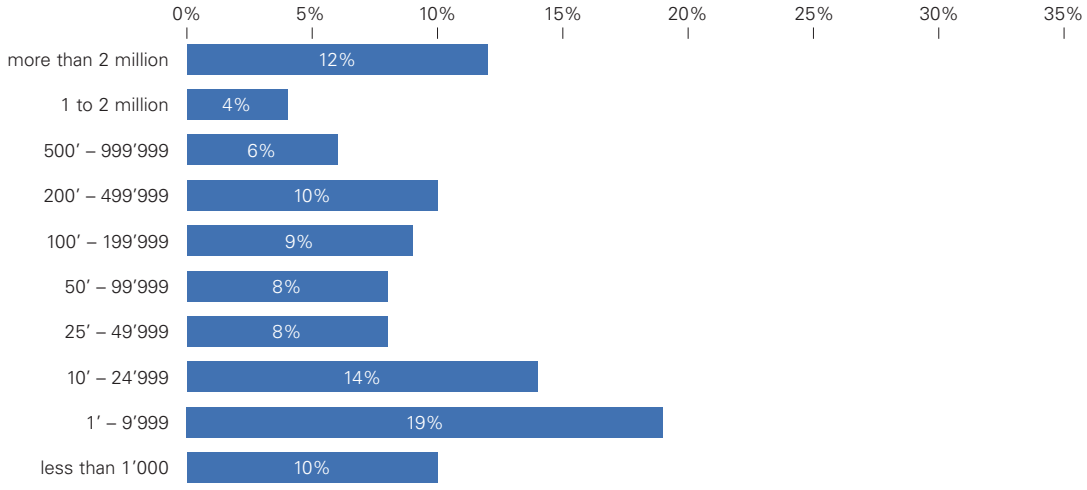
We examined how many fraudulent transactions the perpetrators committed in detail:

Quantity of acts/transactions

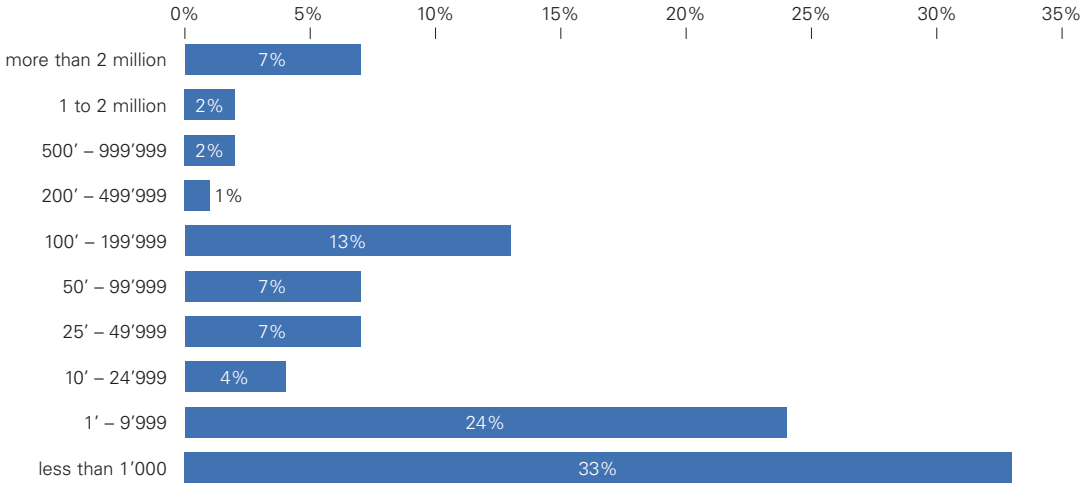


35 percent of fraudsters acted less than 10 times, an additional 33 percent carried out between 10 and 49 fraudulent transactions and 17 percent acted more than 100 times. Consequently: in more than 65 percent of profiles the fraudsters embezzled, stole, deceived, bribed or misappropriated at least 10 times and every third perpetrator acted more than 50 times.

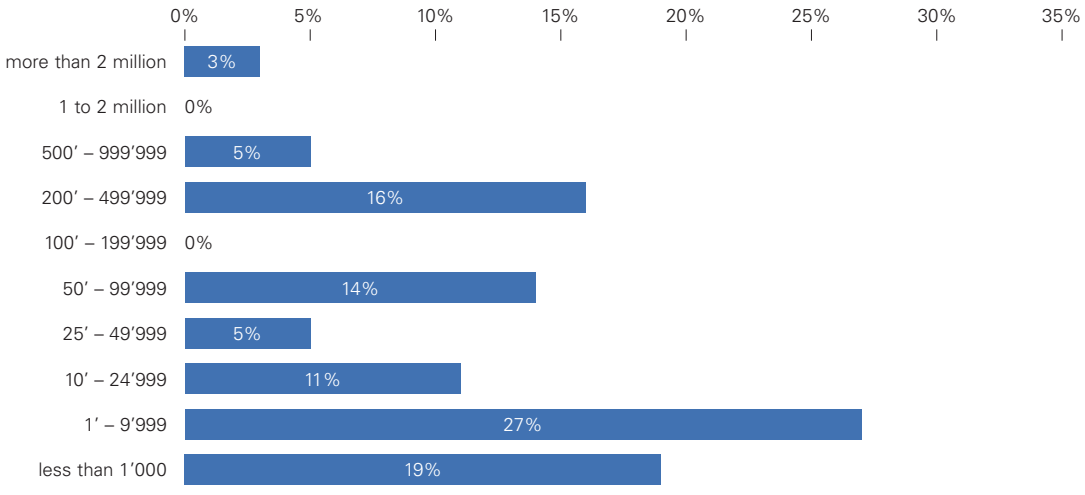
Amount per individual fraudulent act/transaction in Europe



Amount per individual fraudulent act/transaction in South Africa



Amount per individual fraudulent act/transaction in India and the Middle East



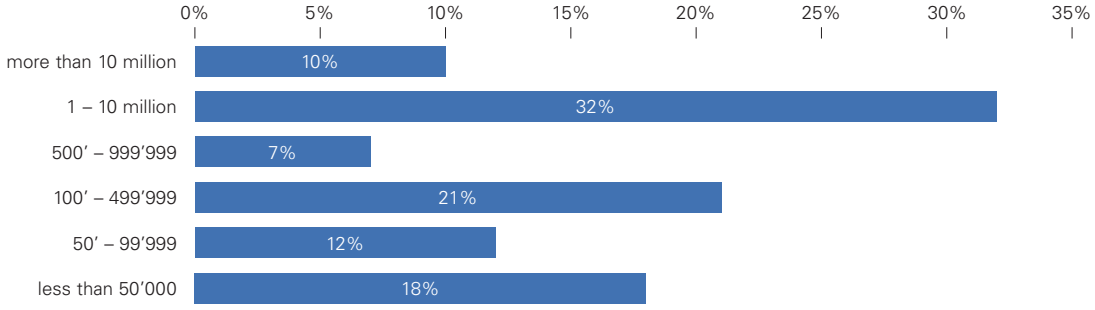
In Europe, India and the Middle East, the loss amount per fraudulent transaction was valued between 1,000 to 25,000 EUR (33 percent and 38 percent respectively). Beyond this, in Europe, results also show a large number of fraudulent transactions valued at over one million EUR (16 percent).

In South Africa, the amount per fraudulent transaction was most commonly less than 1,000 EUR (33 percent), followed by a value between 1,000 and 25,000 EUR (28 percent). Additionally in this region almost every tenth fraudulent act amounted to over one million EURO.

Total loss per profile

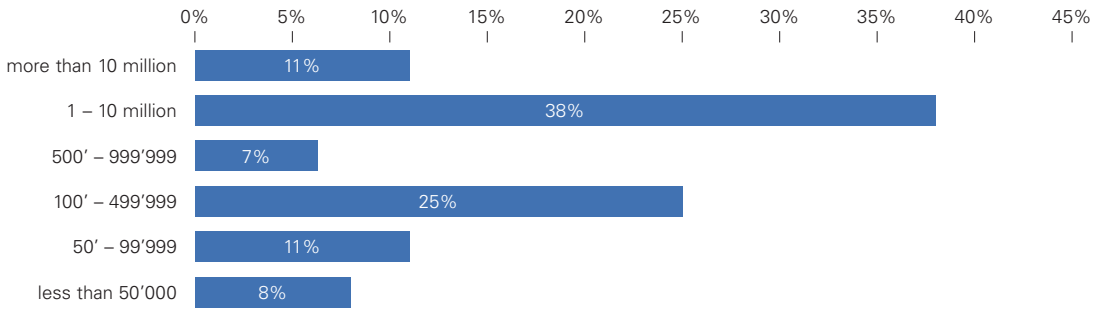
Besides the indirect and immaterial damages, which are difficult to measure or assess, the figures presented in the following two charts focus on the direct total financial loss caused by each fraudster and/or profile.

Total loss in EMA

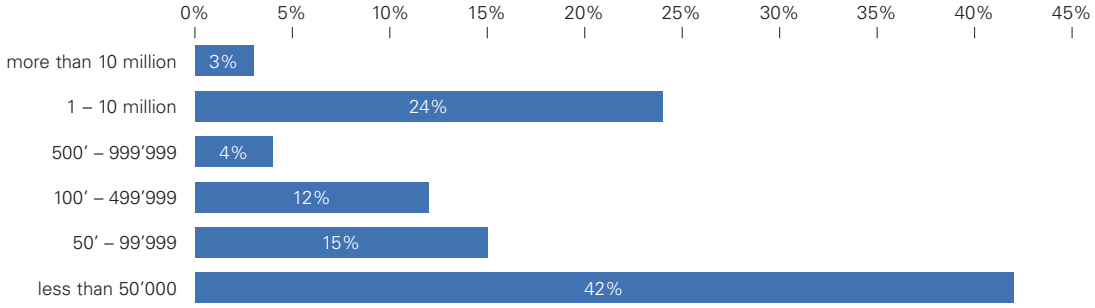


The figures reveal that in 42 percent of profiles the total loss per profile is more than 1 million EUR, but also the category less than 50,000 EUR shows a not insignificant number. To gain a clearer and more detailed overview and to consider the different cultures and regional conditions the figures have been split up into the three regions:

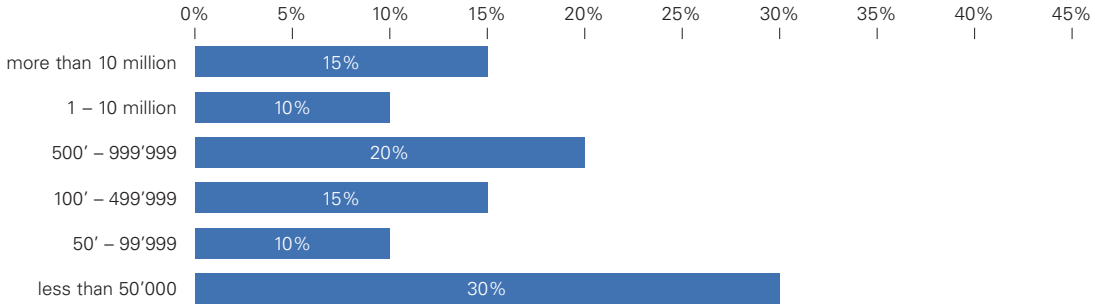
Total loss in Europe



Total loss in South Africa



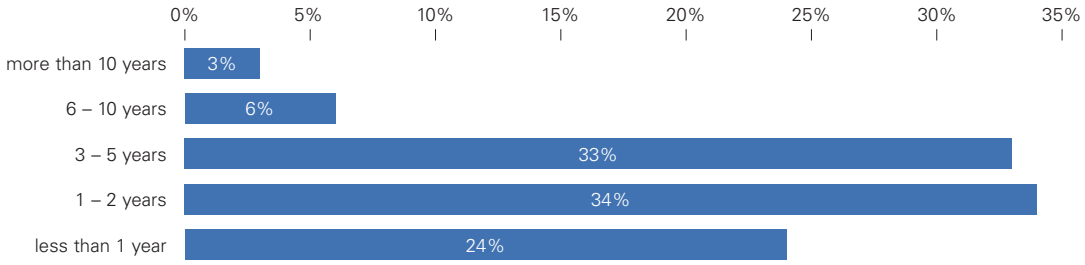
Total loss in India and the Middle East



The total financial direct loss caused by fraudsters and/or per profile and divided into the three regions is as follows: In South Africa, India and the Middle East the total loss per profile is predominantly less than 50,000 EUR (42 percent and 30 percent), this amount plays only a secondary role in Europe (8 percent), where most total losses are in the range of 1 to 10 million EUR (38 percent). Regarding the loss of more than 10 million EUR, India and the Middle East is the region with the greatest number of such losses (15 percent).

A loss of 1 million EUR or more was caused by almost every second fraudster in Europe (49 percent) , by almost every fourth perpetrator in South Africa and in India and the Middle East.

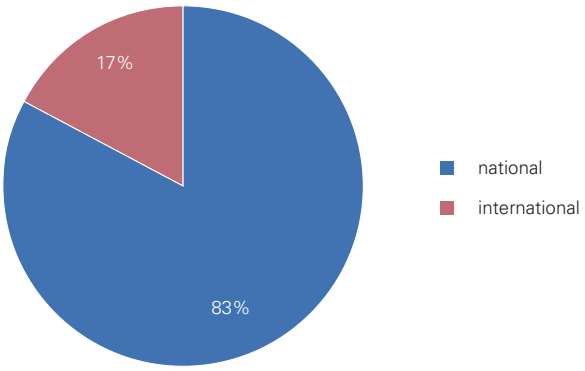
Timeframe – duration from first to last act/transaction or to discovery



In 24 percent of profiles the fraudsters extended their fraudulent acts over or were discovered within a period of less than 1 year. In other words: in more than three quaters of all profiles the existing internal controls seemed to be insufficient to detect the fraud within their normal and yearly scheduled routine.

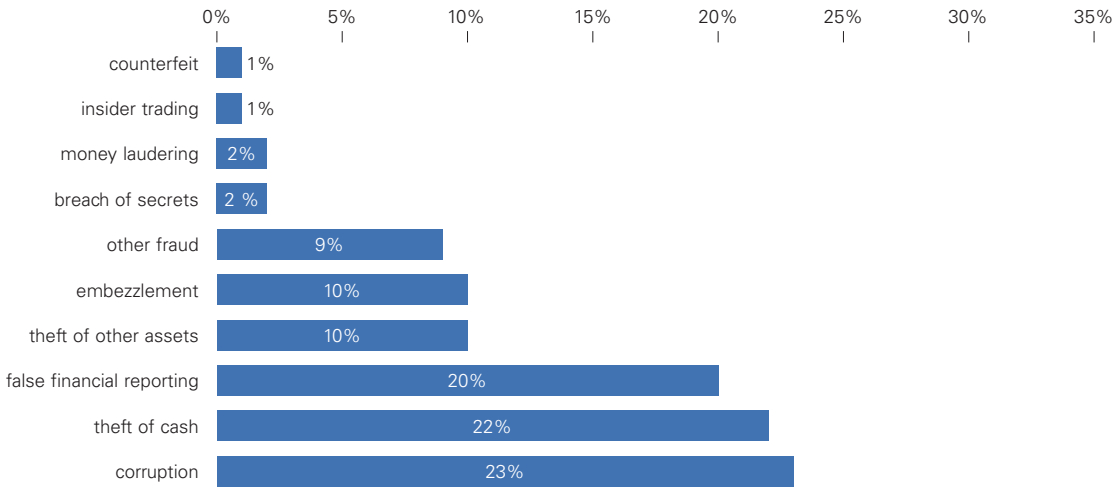
In 34 percent of profiles the perpetrator committed multiple fraudulent acts within the timeframe of 1 to 2 years and in 33 percent of profiles the fraudulent acts lasted over a period of 3 to 5 years. Additionally, almost every tenth offender was able to act for more than 5 years on only detected ofter 5 years. These results highlight the fact that perpetrators were able to continue committing fraudulent acts over a long period of time without detection and hence emphasizes the need for action in the area of fraud risk management.

Location of fraud

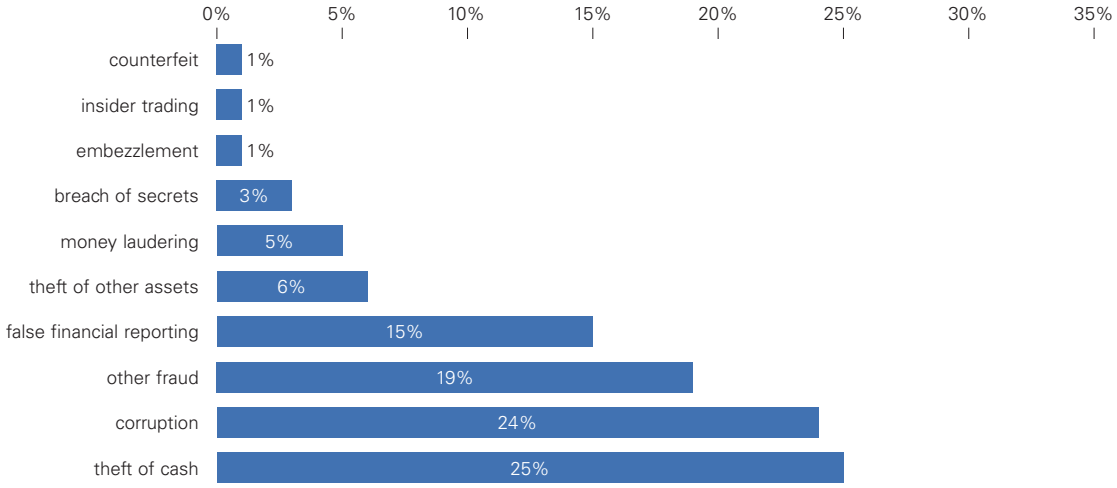


In 83 percent of profiles the perpetrators acted on a national basis. These results could imply that even during this era of globalization and worldwide networks, fraudsters tend to limit their fraudulent acts to local rather than multinational environments.

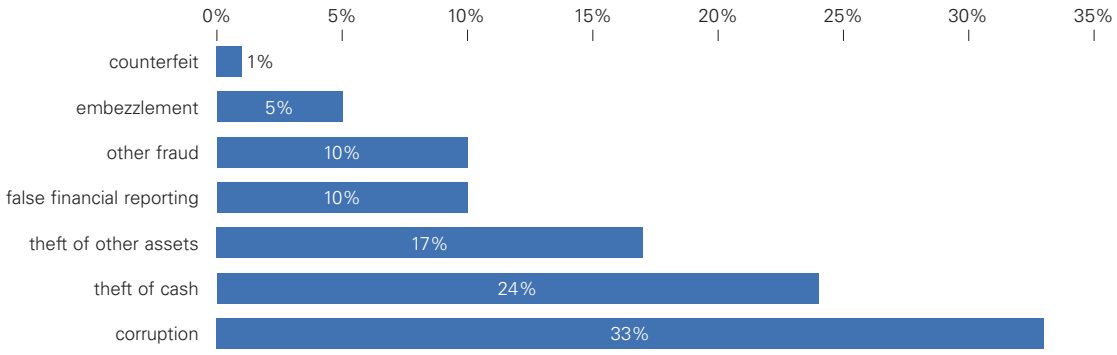
Type of fraud in Europe



Type of fraud in South Africa



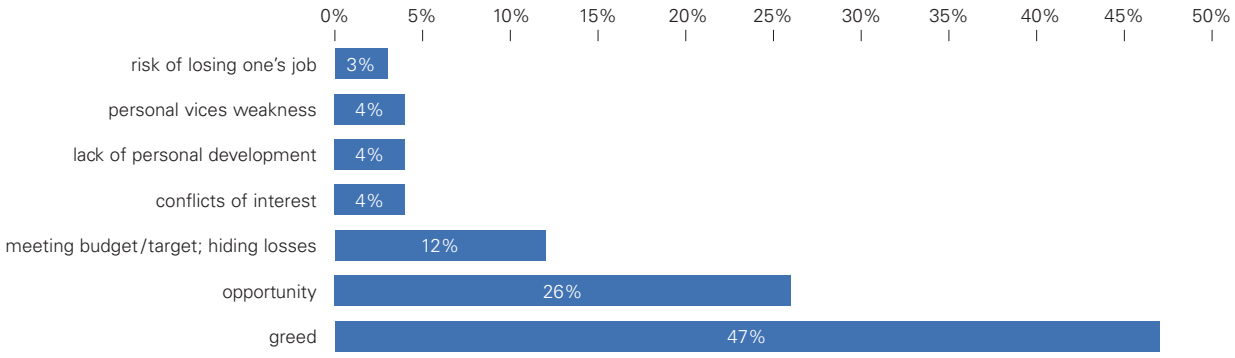
Type of fraud in India and the Middle East



Due to the various jurisdictions involved in this survey, the different types of fraud were broken down by regions. Results indicate that theft of money and other assets was the leading fraudulent act committed by the perpitrators. Additionally, false financial reporting, embezzlement and kickbacks were also significantly common types of fraud that fraudsters committed.

4.3 Other Circumstances

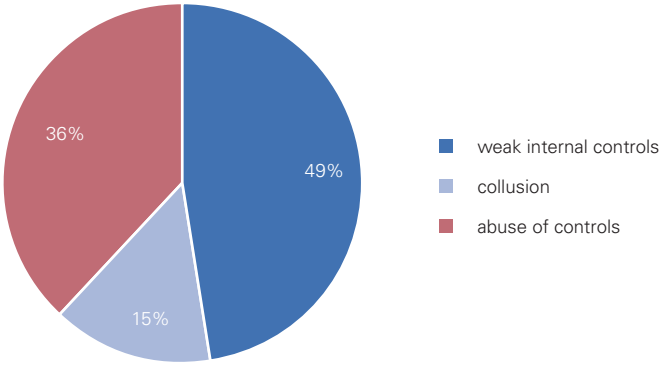
Fraudster's overriding motivation



In nearly half of the profiles, the overriding motivation for committing fraud was greed: perpetrators committed fraud to increase their financial position, power and/or influence. Taking advantage of an opportunity was the second most common fraud motivator and meeting the preset budget/target and hiding losses the third.

What leads a person to become a criminal, to betray someone's trust and to jeopardize his job, career and future? Is this only a result of education and character or are there additional factors influencing this attitude and behavior? Damaged companies should particularly question if their company culture and ethical concept are intact or may rather have provided an appropriate contribution in supporting negative intrinsic motivations.

Conditions that enabled the fraudsters to act

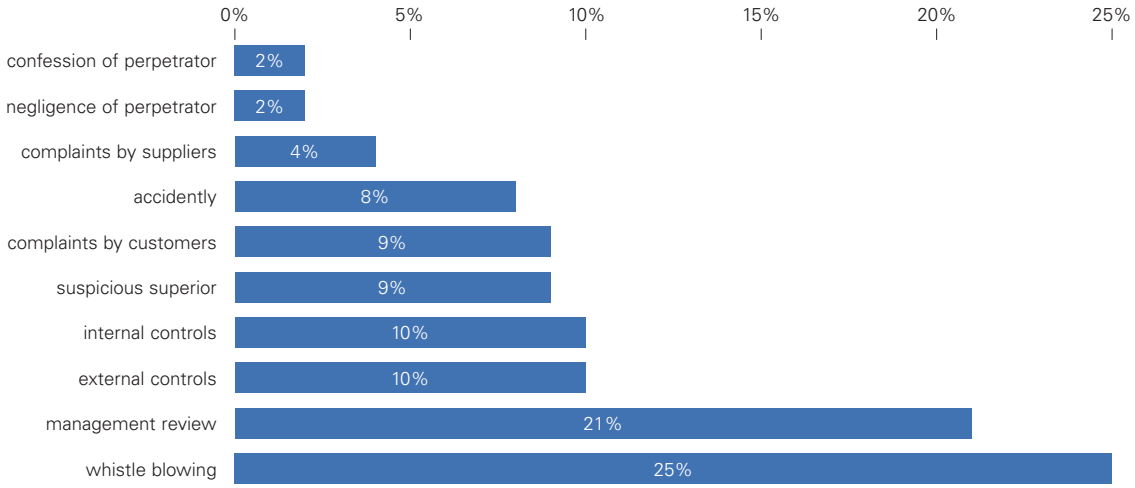


Perpetrators primarily exploited weak internal controls. Additionally, fraudulent acts occurred as a result of perpetrators abusing trust gained from managers and colleagues.

These results highlight the difficult but essential balance that effective internal controls must strike. Sufficient controls must be strong enough to protect company assets but flexible enough to allow business to be conducted efficiently. The fact that in 42 percent of profiles fraud was repeatedly committed over long periods of time indicates that for companies with established internal controls there is still room to further improve their fraud protection mechanisms.

According to the survey results, most fraudsters did not misuse existing controls, but rather took advantage of insufficient controls – in nearly half the profiles. This result should raise questions about the quality of the companies' current fraud risk management policies in place as well as highlight the need for improvement.

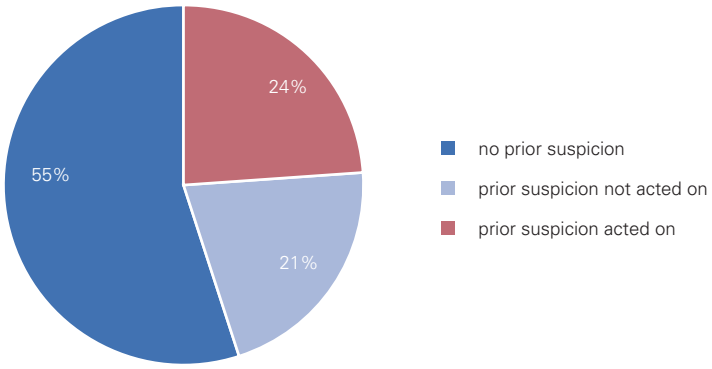
Fraudster detected by



Anonymous tips (whistle blowers) provided the primary source for detection of fraudulent acts. Additionally, management review often led to the detection of fraud. Only 10 percent of all profiles were detected by internal controls. This statement becomes more significant when put into context with the results concerning the conditions allowing the fraud to occur.

While they may not get their hands dirty committing fraud, white collar criminals do leave traces behind. Appropriate follow up of specific fraud warnings and warning signs allows companies to lessen their damages.

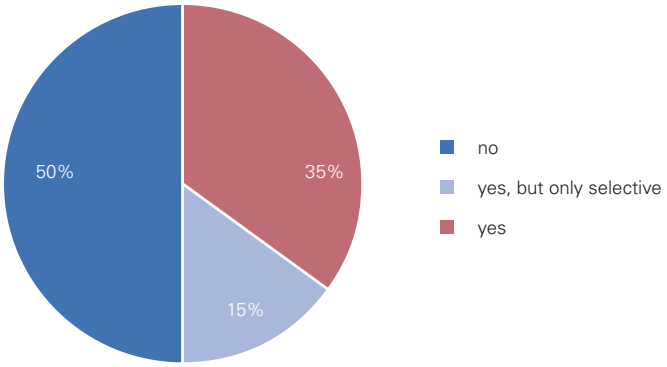
Prior suspicion



In 55 percent of profiles no prior suspicion existed. Notably, in 21 percent of profiles, prior suspicion existed but no follow up action was taken. These results represent a lost opportunity for these companies to mitigate their damages.

5 Fraud Management within the Company

Communication

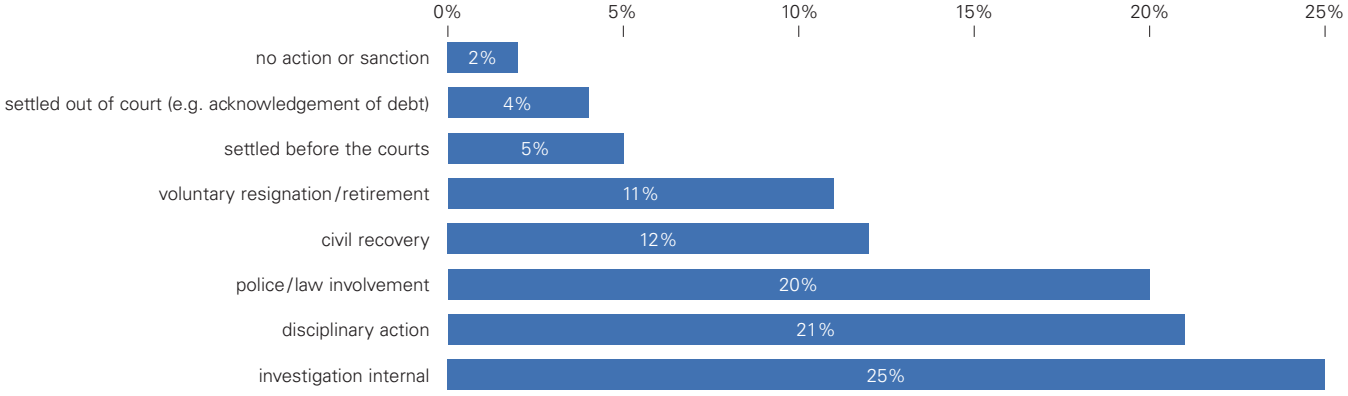


In half of the profiles the offense was neither published nor communicated within the affected company. In 15 percent of profiles the offense was published selectively, meaning either by informing only a select group of people, such as the board, the audit committee, top management, the involved department, and/or by providing only limited and restricted information.

These results raise the issue surrounding affected companies' consideration of the possibility of fraud occurring and their response. An effective ethics and integrity system could have anticipated and planned for such situations. Training and monitoring of ethics and integrity could have diminished the circumstances that gave rise to the fraud risk and created a planned response. "Tone at the top" and "zero tolerance" are terms that need to be applied, trained and monitored.

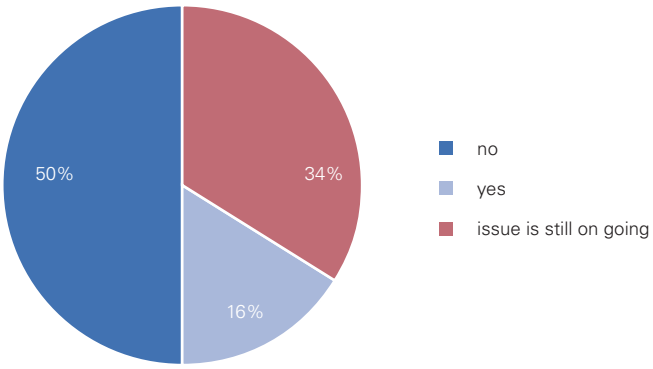
It is critical for companies to have effective policies for following up after experiencing or suspecting fraudulent behavior – and these should include internal and external communication.

Follow up actions



Besides the external investigation conducted by KPMG the companies also carried out internal investigations, took disciplinary or legal actions and/or involved the police. Results revealed that the leading follow up actions were internal investigations, disciplinary actions and the involvement of police and law. Only in 2 percent of all profiles did the companies take no additional action or sanctions.

Asset recovery

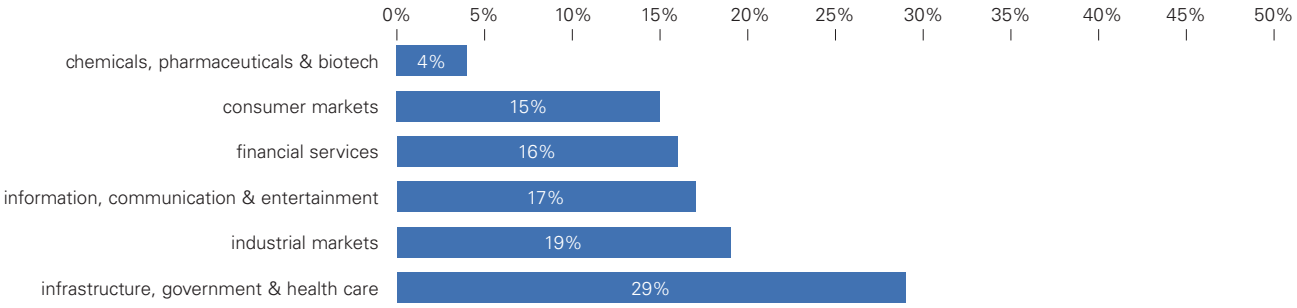


Prevention of fraudulent acts is the best strategy to protect a company and its assets. What are the next steps, if the company has already been damaged? While it is possible to recover stolen assets, it often takes a considerable amount of time and effort on the part of the organization. Results showed that in 16 percent of profiles companies recovered stolen funds. However, in 34 percent of profiles, due to the difficulties of recovering stolen assets, especially with regard to the duration of court proceedings, this issue is still ongoing. In half of the profiles the assets have not been recovered.

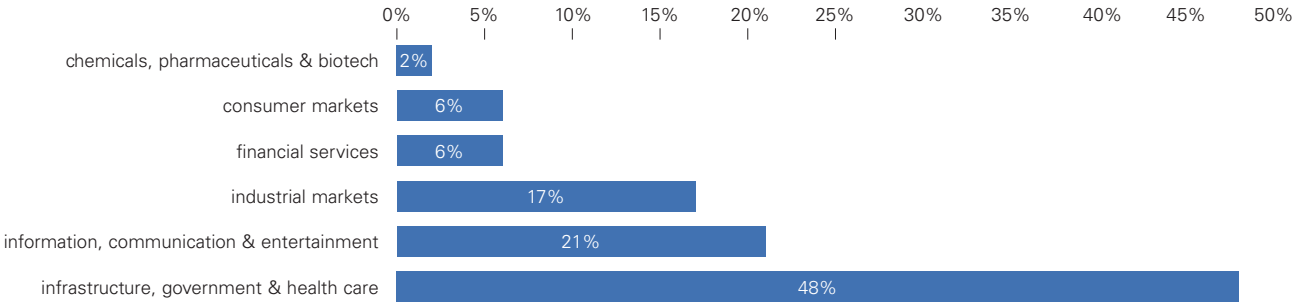
6 Company Facts & Figures

6.1 Branch of victim's organization

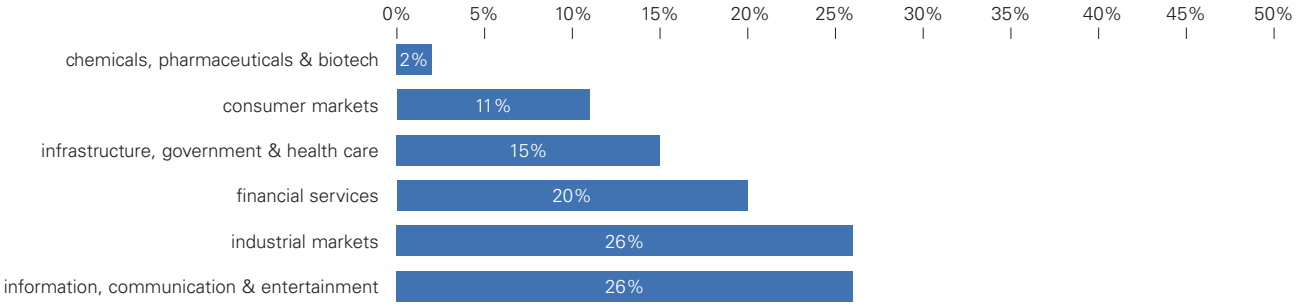
Branch of victim's organization in Europe



Branch of victim's organization in South Africa



Branch of victim's organization in India and the Middle East



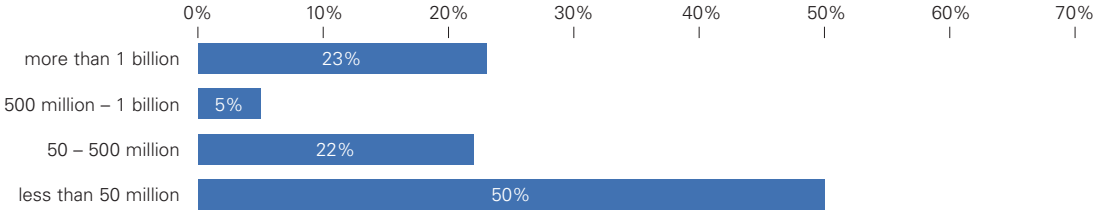
Based on this survey all sectors in Europe are almost equally affected. The infrastructure, government & health care sector, ranked first with 29 percent while the other sections representing second place and following only show a marginal difference at 15 – 19 percent.

In South Africa, fraud is most commonly committed in the infrastructure, government & health care sector, and followed by the information, communication and entertainment sector. The financial services (6 percent), consumer markets (6 percent) and chemicals pharmaceuticals & biotech sector (2 percent) are affected less often.

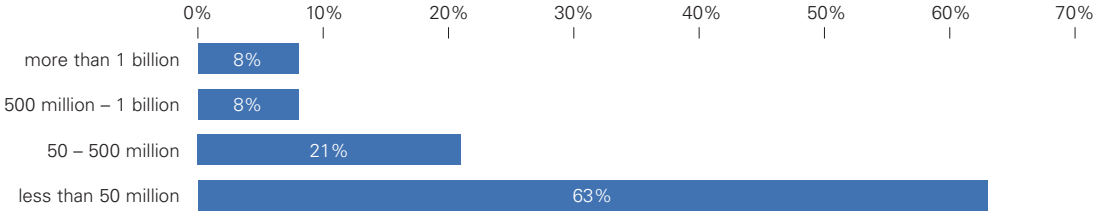
In India and the Middle East fraud is most likely to occur in the information, communications and entertainment sectors and in the industrial markets. Here also the financial sector is the target of fraudulent activities (20 percent).

6.2 Company size

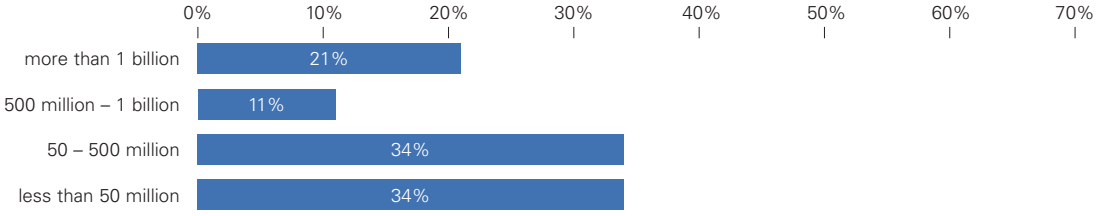
Company size in Europe



Company size in South Africa



Company size in India and the Middle East



The assumption that fraudulent acts primarily occur in large corporations could not be confirmed by the survey results. In fact, they show that small to medium size companies are also at risk. In Europe, in half of the profiles, the turnover was less than 50 million EUR. In South Africa it was even 63 percent.

In India and the Middle East the companies with a turnover of less than 50 million and between 50 and 500 million were affected similarly (in total amounting to 68 percent).

In all three regions the categories were affected the most and the middle-ranking sizes were under represented; whereas in Europe, India and the Middle East the companies with a turnover of more than 1 billion EUR were again more affected.

7 Europe, Middle East and Africa Contacts

KPMG in Austria
Gert Weidinger
Tel. +43 732 6938
gweidinger@kpmg.com

KPMG in Belgium
Els Hostyn
Tel. +32 (0) 2708 4362
ehostyn@kpmg.com

KPMG in Central and Eastern Europe
Jimmy Helm
Tel. +420 222123 430
jhelm@kpmg.com

KPMG in Denmark
Torben Lange
Tel. +45 3818 3184
torbenlange@kpmg.dk

KPMG in France
Jean-Luc Guitera
Tel. +33 (0) 1 5568 6962
jguitera@kpmg.com

KPMG in Germany
Dieter John
Tel. +49 221 2073 1575
djohn@kpmg.com

KPMG in India
Deepankar Sanwalka
Tel. +91 124 2549111
dsanwalka@kpmg.com

KPMG in Ireland
Andrew Brown
Tel. +353 410 11 47
andrew.brown@kpmg.ie

KPMG in Italy
Gabriella Chersicla
Tel. +39 02 6763 2440
gchersicla@kpmg.it

KPMG in Luxembourg
Eric Collard
Tel. +353 2 2 51 51 240
eric.collard@kpmg.lu

KPMG firms in the Middle East
Colin Lobo
Tel. +971 (6) 517 0724
CDJLobo@kpmg.com

KPMG in the Netherlands
Rens Rozekrans
Tel. +31 20 656 7781
Rozekrans.Rens@kpmg.nl

KPMG in Russia
Ian Colebourne
Tel. +7 495 937 2524
Ian.Colebourne@kpmg.com

KPMG in South Africa
Petrus Marais
Tel. +27 214 087 022
pmarais@kpmg.com

KPMG in Spain
Pablo Bernad
Tel. +34 91 456 3400
pablobernad@kpmg.es

KPMG in Sweden
Martin Kruger
Tel. +46 (0) 8723 9199
martin.kruger@kpmg.se

KPMG in Switzerland
Anne van Heerden
Tel. +41 44 249 31 78
annevanheerden@kpmg.com

KPMG in the UK
Adam Bates
Tel. +44 (0) 20 7311 3934
adam.bates@kpmg.co.uk

kpmg.com