



*cutting through complexity™*

KPMG ANALYSIS OF GLOBAL  
PATTERNS OF FRAUD

# Who is the typical fraudster?

[kpmg.com](https://www.kpmg.com)



# Contents

Introduction	<b>1</b>
Methodology	<b>2</b>
What our analysis revealed	<b>3</b>
Motivations for fraud	<b>9</b>
Warning signs	<b>13</b>
Size of the crime	<b>15</b>
Duration of fraud	<b>16</b>
Raising awareness	<b>18</b>
Fraud is up; defenses are down	<b>21</b>
Red flags not to be missed	<b>22</b>
Further guidance on how to keep your business safe	<b>23</b>

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2011 KPMG International Cooperative (“KPMG International”), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

All rights reserved.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.

KPMG Forensic is a service mark of KPMG International.

# Introduction

Who is the typical fraudster? Are there any defining features, traits, or behaviors that could help you to identify those individuals within your organization more likely to perpetrate fraud?



## If only it were that simple

KPMG's 2011 global analysis of fraud trends can help you to draw inferences. We have narrowed down the profile of a typical fraudster, based on scrutiny of actual instances of fraud, to help organizations like yours become more alert and responsive to fraud.

KPMG International's 2011 study follows our 2007 analysis of fraudulent behaviors within the Europe, Middle East, and Africa region (EMA). Our last report proved so popular that we have now extended our analysis worldwide. We have sought to identify patterns among individuals who have committed acts of fraud and contrasted the value and duration as well as many other characteristics.

Our research is based on 348 actual fraud investigations conducted by KPMG member firms in 69 countries. While it includes some high-profile reported cases of fraud, for the most part, these investigations were not publicized. The sample is very broad in the size and scope of fraud committed and is far-reaching in terms of the sectors and geographies covered.

## Here is what we found out about the typical fraudster:

- Male
- 36 to 45 years old
- Commits fraud against his own employer
- Works in the finance function or in a finance-related role
- Holds a senior management position
- Employed by the company for more than 10 years
- Works in collusion with another perpetrator

As in 2007, unsurprisingly, the overriding motivation for fraud is personal greed, followed by pressures on individuals to reach tough profit and budget targets. The survey highlights, more importantly, how weakening control structures make the opportunity to commit fraud easier. Organizations should take some of the blame. For them, it is time to consider how they contribute to fraud when failing to detect or respond to lapses or gaps in controls, or by setting overly onerous targets.

Read on to find out more about the potential fraudsters. Discover which "red flags" to look out for and how to implement more effective measures to manage the prevention and detection of fraud and your response to it.

### Phillip D. Ostwalt

Global and Americas Investigations Network Leader

### Richard Powell

EMA Investigations Network Leader

### Mark Leishman

ASPAC Investigations Network Leader

# Methodology

KPMG gathered data and details from fraud investigations conducted by our firms' forensic specialists in EMA, the Americas, and Asia Pacific from January 2008 to December 2010. In all, 348 cases from 69 countries were analyzed.



## White collar crimes

From the thousands of fraud investigations conducted by KPMG Forensic<sup>SM</sup>, data has been collated relating to a sample comprising "white collar" crimes with a clear perpetrator. The frauds included in this analysis comprise material misstatement of financial results, theft of cash and/or other assets, abuse of expenses, and a range of other fraudulent acts.

Excluded from the sample are frauds considered to be of no material value, acts of misconduct or those where fraud could not be substantiated during the investigation, as well as cases lacking sufficient detail.

## The analysis identifies:

- Fraudster profiles and details of more common types of fraud
- Conditions that tend to enable fraud
- Typical follow-up actions by organizations impacted by fraud

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

This report does not reveal the names of parties involved, in order to protect confidentiality. Many of the cases included here did not reach the public domain; others reported only headline details of the fraud. This is fairly typical in our experience.

All monetary values are expressed in U.S. dollars.

# What our analysis revealed

Typically, a fraudster is perceived as someone who is greedy and deceitful by nature. However, as this analysis reveals, many fraudsters work within entities for several years without committing any fraud, before an influencing factor—financial worries, job dissatisfaction, aggressive targets, or simply an opportunity to commit fraud—tips the balance. Here's what we found.



## Individual profile

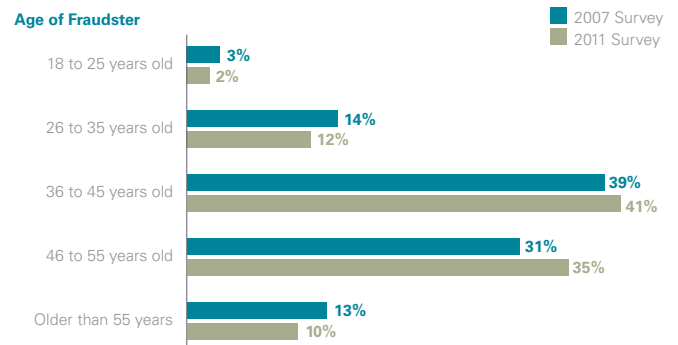
### Age

Our survey finds that the typical fraudster is between the ages of 36 and 45. This group rose from 39 percent of cases in 2007 to 41 percent in 2011. This is closely followed by a group accounting for 35 percent of fraudsters who were between 46 and 55 years old.

### Gender

While men were found to be more likely perpetrators of detected fraud (85 percent in 2007 and 87 percent in the 2011 analysis), women in the Americas (22 percent) and Asia Pacific (23 percent) are almost three times more likely to be involved in fraud than in EMA (8 percent). This might be due, perhaps, to fewer women in senior positions in "old Europe" and Africa compared with other regions of the world.

The survey's finding that men commit more fraud than women seems a reflection on the gender make-up of companies generally. The gender gap in fraud perpetration may reflect women's under-representation in senior management positions and, as a consequence, fewer opportunities to commit fraud.

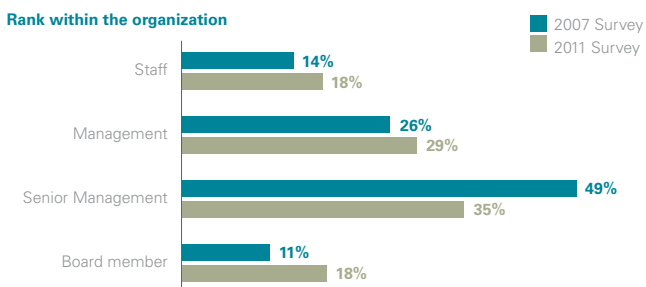




### Rank within the organization

Within the fraud matters we analyzed, we found the people most often entrusted with a company’s sensitive information and able to override controls are statistically more likely to become perpetrators. This is borne out by survey evidence that senior management is more frequently implicated in fraud than junior staff.

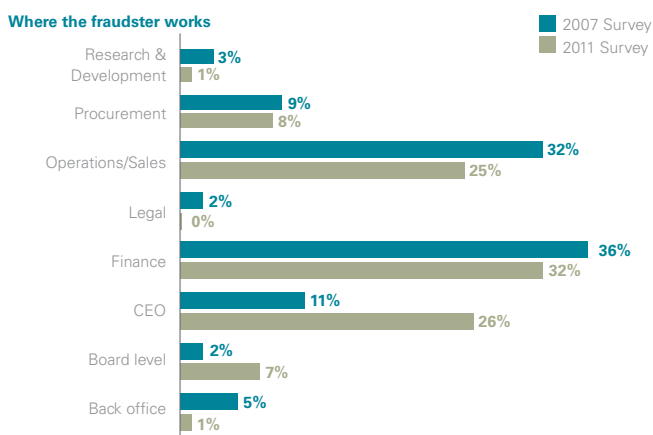
In 2007, the EMA survey found that 49 percent of all fraudsters held senior management positions. While senior managers remain the most likely fraudsters according to the 2011 analysis, the overall percentage fell to 35 percent. Conversely, however, board level perpetrators increased from 11 percent to 18 percent between 2007 and 2011.



### Where the fraudster works

The survey finds that most people involved in committing fraud work in the finance function—36 percent in 2011 compared with 32 percent in 2007. Access to and responsibility for corporate assets, financial reporting, and credit lines all offer significant temptation and opportunity to commit and conceal acts of fraud.

After finance, fraudsters are most likely to work in the chief executive’s/managing director’s office (26 percent up from 11 percent in 2007) or in operations and sales (25 percent in 2011 down from 32 percent in 2007). Employees in the legal function continue to be the least likely perpetrators.



# View from Central and Eastern Europe

## How does the global survey reflect regional findings?

*"In Central and Eastern Europe (CEE), many multinational companies have tended to transfer trusted expatriate employees from the parent company into key financial positions at their subsidiaries in the region, to provide not only the necessary experience, but also to "police" the subsidiary from within the finance function. They act as whistleblowers, the initiators of investigations. Often they are further transferred from region to region as the company sets up new operations to ensure the ongoing integrity of the finance function,"* says KPMG's head of Forensic in CEE, Jimmy Helm.

The region therefore bucks the global trend. Fewer frauds occur within the finance function, while most are committed within sales and procurement. Collusion with third parties—clients and suppliers—is evident in many fraud cases in the region.

Helm comments: *"Lack of trust in local regulatory and judicial systems often results in affording the perpetrators an opportunity to resign without the offense going to court or becoming public. Consequently HR references are unable to address the disciplinary issues, and poor background checking allows these fraudsters to re-enter the business community."*

### Most interesting fraud investigation

In 2010, the Forensic practice in CEE was engaged by a foreign-listed client to investigate irregularities at a subsidiary in CEE too small to warrant a separate financial audit. The investigation found that local management (the general manager and financial

controller) falsified financial records for more than five years.

- Turnover was boosted (in some years by as much as 70 percent) by fictitious customer contracts, while payments were made to fictitious suppliers. Funds were continually recycled to create false revenue that kept the company going.
- The parent company invested further cash into the business under the illusion that it was operationally sound and securing contracts.
- Further funds were misappropriated for the personal use of the general manager and financial controller.
- The subsidiary had actually lost its license to trade in 2007 in a key market but had concealed this from the parent company.

The general manager and financial controller were dismissed and criminal and civil charges brought against them. The client further engaged KPMG to restate the subsidiary's financial records back to 2005, to support disclosures to the relevant stock exchange and to make appropriate financial adjustments to the parent company's financial statements.

Helm is responsible for KPMG's services in the 18 former Soviet-bloc countries. Based in Prague in the Czech Republic for the past 11 years, he was formerly a senior prosecutor of white-collar crimes in the High Courts in South Africa. Helm has 17 years' experience in leading fraud, misconduct, and bribery/corruption investigations. In addition to heading up investigations, he advises clients on fraud risk strategies and on anti-bribery and corruption initiatives.

### Contact Jimmy Helm:

+420 222 123 430

[jhelm@kpmg.com](mailto:jhelm@kpmg.com)

“Lack of trust in local regulatory and judicial systems often results in affording the perpetrators an opportunity to resign without the offense going to court or becoming public.”

comments Jimmy Helm



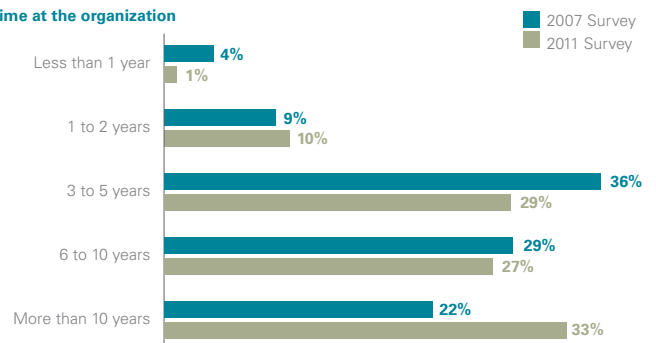
### Time at the organization

In 2007, 36 percent of fraudsters were likely to have worked at a company for between three and five years before detection of the fraud. In 51 percent of cases, they worked at the company for more than five years and, in 22 percent of cases, for more than ten years.

In 2011, the analysis shows an increase in the detection of fraud among longer-term employees. It reveals that 60 percent of fraudsters worked at the company for more than five years before the fraud was detected, while 33 percent of fraudsters worked there for more than ten years.

Given that fraudsters usually work for their employer for over five years before discovery, whereas the average fraud has occurred for just over three years by the time of its discovery, it is plausible that those who commit fraud often do not join organizations with the intent to commit fraud. However, changes in personal circumstances or pressures to meet aggressive work targets may influence the onset of fraudulent activity. They may then commit fraud once they have their feet comfortably under the table, when they have gained the trust and respect of colleagues and have identified weak controls and opportunities to exploit the business.

Time at the organization



“Organizations need to recognize that fraud does happen. With a robust compliance program and protocols for prevention, detection, and response, they will be better able to deal with it and move on.”

explains Graham Murphy

## View from the United States

### How does the global survey reflect regional findings?

In the United States, the archetypal fraudster closely mirrors the profile identified in the global survey: male, senior executive, long-term employee. *“We find the higher the level of executive, the greater the value of the fraud. Greater oversight responsibility often offers greater opportunity for bigger frauds,”* explains Graham Murphy, who heads up KPMG’s Forensic Services practice in the U.S. firm’s Midwest region.

Detection of fraud involving collusion with outside parties has increased significantly in U.S.-based companies in recent years. Murphy attributes this in part to anti-bribery and corruption initiatives—notably the Foreign Corrupt Practices Act (FCPA)—and task forces designed to clamp down on misconduct.

*“More and more of these cases are coming to light because of increased enforcement capabilities,”* he explains. *“Corporate America is becoming very focused on this issue as companies build out their compliance programs and enhance their awareness of and responses to fraud and misconduct.”*

As fraudsters are often one or two steps ahead of compliance programs, Murphy stresses the need for organizations to understand their vulnerabilities, to patch holes in their defenses when detected, and to look proactively for red flags and other indicators of fraud.

*“Organizations need to recognize that fraud does happen. With a robust compliance program and protocols for prevention, detection, and response, they will be better able to deal with it and move on.”*

### Most interesting fraud investigation

At a U.S. financial institution, a larger-than-life chief executive surrounded himself with an inner circle of “yes men.” The fraud, which involved subterfuge and complex bundling and unbundling of loans and transactions to make bad loans appear good, was exposed in part by the dwindling value of collateral and related property values in an eroding economy.

The investigation quickly uncovered conflicting stories told by the CEO’s inner circle and the people working with the loans and customers. This case illustrates, in particular, how dominant and bullying behavior can coerce others to participate in fraudulent activity.

Lessons are learned from investigations such as this. Increased knowledge, and tools developed to uncover such schemes, can be transferred to other financial institutions to seek out proactively weaknesses in their internal processes and controls so that they can fortify their own compliance programs. Specifically, tools have been developed to provide better insight into loan portfolios and more proactive identification of bad loans and potentially fraudulent activity.

Following a period of regulatory oversight, another financial institution took over certain of the bank’s assets.

Graham Murphy leads the U.S. firm’s Midwest Forensic practice. Since 1991, his experience crosses Europe, Asia, and North and South America and includes financial investigations involving earnings manipulation, accounting irregularities, theft and misappropriation of assets, and conflict-of-interest issues. He has provided testimony to the Securities & Exchange Commission (SEC) and has appeared as an expert witness in fraud cases.

### Contact Graham Murphy:

+1 312 665 1840

[grahammurphy@kpmg.com](mailto:grahammurphy@kpmg.com)

“We find that most fraud continues to be committed at senior and middle-management levels.”

explains Anne van Heerden

## View from Switzerland

### How does the global survey reflect regional findings?

“We find that most fraud continues to be committed at senior and middle-management levels,” says Anne van Heerden, head of Forensic at KPMG in Switzerland. “More frequently, collusion with external parties is also evident—notably among suppliers who over charge for their services and give a kick-back to the internal perpetrator.”

Switzerland is renowned for its financial services industry and it is here where many fraudsters operate. “Fraudsters attempt to extract money from dormant accounts or they assume the identity of a customer to trick advisers into making payments or transfers. Often this involves the collusion of an external party with an internal ally,” explains van Heerden.

Family offices in Switzerland are also becoming targets for fraudsters. Submissions of fraudulent invoices by suppliers, or flawed investment activities, are among the most typical frauds. Perpetrators tend to be employees and outside agents such as investment advisers rather than family members.

### Going solo or in collaboration?

In 2007, 69 percent of perpetrators were employed by the organization they defrauded. This rose massively to 90 percent in the 2011 global survey.

There has also been a dramatic increase in the likelihood of collusion—almost doubling from 32 percent of perpetrators in 2007 to 61 percent in 2011. By definition, collusive activity is harder to detect as it involves circumvention of the control system by two or more parties.

Where colluding parties are external to, rather than employed by, the defrauded entity, these are most commonly suppliers (48 percent) and customers (22 percent), according to the 2011 analysis. Consultants and sub contractors make up the majority of the balance.

In parts of EMA, the analysis reveals a more marked pattern of collusion between employees and suppliers of the victim organization than elsewhere in the world.

### Most interesting fraud investigation

KPMG in Switzerland is helping to resolve a case involving an individual who invested heavily into a business for more than ten years. When he failed to receive dividends and returns on his investment and needed to make tax declarations, he hired KPMG to undertake a high-level audit.

“The client had been led to believe that he was one of a number of investors. However it soon became apparent that he was the sole creditor to the business. His investments were certainly not working for his benefit” explains van Heerden. “That is when KPMG Forensic became involved. The fraudsters had siphoned off the client’s money over a number of years to fund their extravagant lifestyles.”

Anne van Heerden is head of Forensic, Risk and Compliance at KPMG in Switzerland. Working with KPMG since 1986, he has led many national and international economic crime investigations across several industry sectors. His cases include procurement fraud, manipulation of financial statements and other financial irregularities, tax fraud, bribery, as well as misuse of position and funds, often across multiple borders.

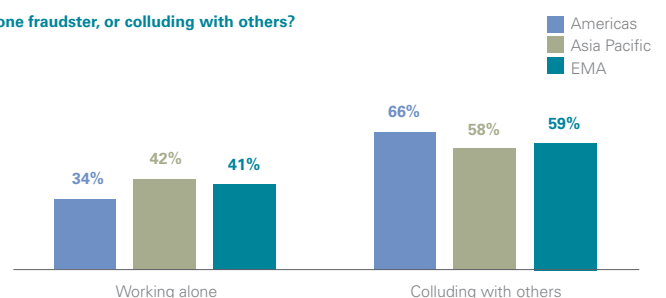
### Contact Anne van Heerden:

+41 44 249 31 78

[annevanheerden@kpmg.com](mailto:annevanheerden@kpmg.com)

Interestingly, the survey finds that male perpetrators (64 percent) are almost twice more likely to collude than women (33 percent). After taking account of male dominance in the perpetrator group, collusive females account for just 4 percent of activity. Perpetrator groups are most typically all-male or mixed gender.

### Lone fraudster, or colluding with others?



# Motivations for fraud

The desire for personal financial gain, directly or indirectly, continues to be the biggest driver of fraud according to the survey.



## Greed and work pressures

Attempts to conceal losses or poor performance (possibly due to pressures to meet budgets and targets, to enhance bonuses, or to safeguard against loss of employment) provide motivation for many frauds, notably those involving the misreporting of results.

Misappropriation of assets, notably due to embezzlement and procurement fraud, accounted for 43 percent of the frauds surveyed in 2011. This echoes the findings in 2007. In second place is fraudulent financial reporting, which again raises concerns about the pressures placed on management to achieve targets.

Companies that fall victim to misreporting and other types of fraud should consider whether they set too onerous targets and exert excessive pressure on employees to achieve them. Faced with criticism about underperformance or concerned by the threat of a reduced bonus or loss of employment, staff might be tempted to hype up their performance by misstating results or to guard against potential financial hardship by defrauding the business.

There tends to be less fraud in companies that make intolerance of fraud part of the corporate culture and which set realistic and achievable targets for employees. It is important, however, that the corporate culture is cascaded across the organization by management who act, at all times, in accordance with the corporate values.

Entities, though they can control their own cultures, are subject to outside influences on employees. In particular, organizations should be mindful of the impact of mounting personal financial pressures on employees due to the global economic crisis. In more austere times, formerly trustworthy employees affected by adverse changes in their personal circumstances might be more tempted to commit fraud when they spot an opportunity.

Given that in the frauds we analyzed that it took, on average, nearly three and a half years between fraud inception and detection, it seems that there may be a significant increase in newly detected cases over the next few years due to current and recent increased financial hardship.

One of the most significant findings of this survey is the very large increase in cases involving the exploitation of weak internal controls by fraudsters – up from 49 percent in 2007 to 74 percent in 2011.



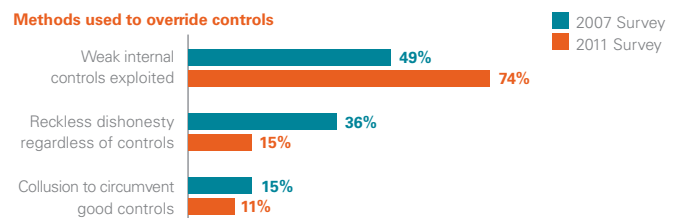
### Gaps in defenses

One of the most significant findings of this survey is the very large increase in cases involving the exploitation of weak internal controls by fraudsters—up from 49 percent in 2007 to 74 percent in 2011.

The difficult economic climate may be partially to blame. Tighter budgets are forcing some companies to cut costs in their control environments. Less robust controls, and fewer resources to monitor controls, allow for greater exploitation by fraudsters. Although necessary to preserve profits, such cost cutting should be balanced with effective risk management.

Many frauds continue to be exposed by formal or informal whistleblowing mechanisms. In 2007, companies were alerted to fraud by whistleblowers in one-quarter of cases, with complaints from customers or suppliers accounting for a further 13 percent. In 2011, formal internal whistleblower reports accounted for 10 percent of detections while anonymous tip-offs were responsible for uncovering 14 percent of frauds. A further 8 percent of frauds were identified due to customer or supplier complaints while 6 percent came in response to issues raised by third parties, including banks, tax authorities, regulators, competitors, or investors.

That one in seven frauds is now discovered by chance puts question marks over the effectiveness of controls and management review at detecting and preventing fraud. In 2007, 8 percent of frauds were discovered by accident, rising to 13 percent in 2011. The upshot is that companies seem to depend increasingly on the good consciences of staff or third parties, on accidental discovery or, in a few cases, on confessions, to identify potential fraud. In aggregate, these methods account for detection in just over half of the frauds in the 2011 survey.





It is highly likely, therefore, that many known instances of fraud go unreported. This may be due to staff's unwillingness to report colleagues, to third parties' reluctance to make a complaint, or because individuals conclude it is unnecessary to raise a particular issue. Individuals often argue that it is not their place to provide tip-offs; others fear repercussions, such as the loss of their job, especially where the fraud involves line or senior managers or board members.

Globally, there are moves to create more formal frameworks to promote whistleblowing. Such initiatives are intended to create more secure environments in which to tip-off. In the United States, for instance, the Dodd-Frank Act (2010) intends to award whistleblowers a bounty worth between 10 percent and 30 percent of fines levied for financial misconduct. In some parts of the world, there are long-standing protections for whistleblowers. In the United Kingdom, for example, the Public Interest Disclosure Act (1998) protects workers who blow the whistle where there is reasonable belief that a crime has been committed.

Such incentives and protections can be helpful, but the fact remains that informal or formal whistleblowing should not be relied upon as principal detection tools.

“Initial red flags are now raised more frequently than ever before, yet responses to these early warning signs have fallen significantly. ”

says Richard Powell

## View from EMA

### How does the global survey reflect regional findings?

Causing concern in EMA is the relative infrequency with which formal control environments and management oversight detect fraud.

Richard Powell leads KPMG’s Investigations Network in the EMA region. *“Many of the frauds I’ve investigated in the past few years have come to light due to formal or informal whistleblowing reports,”* he says. *“Very few, by contrast, are discovered as a direct consequence of management, internal, or external audit review.”*

The importance of annual fraud risk assessments cannot, in Powell’s view, be underestimated. *“Properly conducted and focused risk assessments are an opportunity to identify areas where there are enhanced fraud risks but ineffective or missing controls. Remedial action can then be taken to close the gap and to mitigate the risk of fraud.”*

Although companies in EMA have opportunities to stop fraud before it escalates, red flags are often misunderstood or inappropriately actioned. The fraud typically lasts longer, losses accumulate, and the costs associated with remediation increase. *“Perhaps the most damning finding of the survey is that initial red flags are now raised more frequently than ever before, yet responses to these early warning signs have fallen significantly. Every ignored red flag is potentially a missed opportunity to stop fraud.”*

### Most interesting fraud investigation

A recent whistleblower case in EMA highlighted precisely why companies should create a culture in which individuals feel empowered to raise concerns.

An employee only blew the whistle on a manager when he perceived that disregard of health and safety procedures had endangered the life of a colleague. It emerged, in the course of the investigation, that the individual had also been aware of financial impropriety by the same manager for more than a year. He failed to report those concerns until the health and safety issue tipped the balance. In his opinion, the health and safety issue was a serious matter to be addressed, while the financial fraud was “only company money”.

This whistleblower’s response suggests that financial impropriety was lower on his radar in terms of illegal or inappropriate activity. Only by raising the profile of what constitutes impropriety, by creating a culture that is intolerant of fraud and where employees feel able to raise concerns—regardless of their nature—can such reporting mechanisms become effective deterrents against fraud.

Richard Powell leads KPMG’s Investigations Network in the EMA region. An experienced forensic partner, specializing in fraud and impropriety, Powell also advises KPMG firms’ public and private sector clients on project and program controls, performance improvement, and contract compliance on major construction and infrastructure projects.

#### Contact Richard Powell:

+44 161 246 4044

[richardfa.powell@kpmg.co.uk](mailto:richardfa.powell@kpmg.co.uk)

# Warning Signs

A red flag is an event or set of circumstances that ought to alert an entity to the presence of risk. Within the organization, individuals need to be alert to red flags—what to look out for, how to respond, how to follow-up. By responding appropriately to red flags, fraud can be detected sooner and, in some cases, prevented altogether.



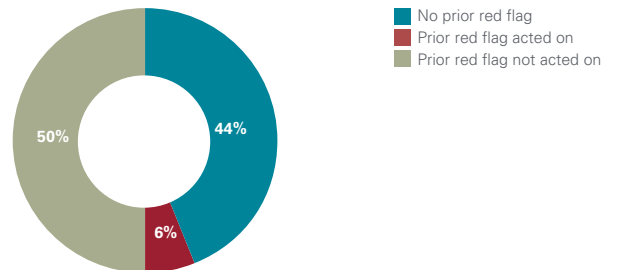
But how often is anything done about a red flag? The number of fraud cases preceded by a red flag rose to 56 percent of cases in 2011, from 45 percent in 2007. However, instances where action was taken following the initial red flag fell massively. Just 6 percent of initial red flags were acted on in the 2011 analysis, compared with almost one-quarter (24 percent) in 2007.

Companies are failing to read and to act quickly on the warning signs. Ignored red flags are a license for perpetrators to carry on operating and a missed opportunity for the business to detect or prevent fraud and to reduce losses and associated costs. Find out which ones your organization needs to address in our guide to red flags on page 22 of this publication.

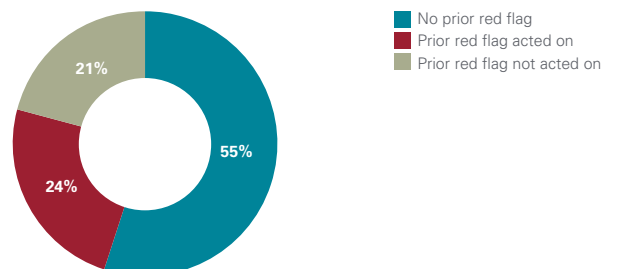
Rarely is an act of fraud a one-off. With financial statement fraud, for instance, fraudsters often make multiple transactions to cover their tracks. In 2007, 91 percent of fraudsters were repeatedly fraudulent, compared with 96 percent in the 2011 analysis.

Repeated and long-running fraudulent activity may result in several red flags over a period. Recognizing and being alert to red flags and responding appropriately could save significant loss of value to the organization from fraud.

Red flags identified and resulting actions taken (2011 Survey)



Red flags identified and resulting actions taken (2007 Survey)



“When frauds blow up, it’s typically several years down the line, when the value of the deception has multiplied and all the warning signs have been missed.”

says Rohit Mahajan

## View from India

### How does the global survey reflect regional findings?

*“The global survey is a good reflection of what is going on in India,”* says Rohit Mahajan, executive director of KPMG’s Forensic practice in India.

*“The value of fraud keeps going up in Asia Pacific and that, I believe, is because the economy is booming here. However, companies are too focused on the front end (growing the business) rather than the back end (the support functions) so red flags get ignored or treated as one-offs. When frauds blow up, it’s typically several years down the line, when the value of the deception has multiplied and all the warning signs have been missed.”*

The global survey found that fraud in Asia Pacific tends to take longer to detect than anywhere else in the world.

Mahajan points out that few companies pursue legal remedy when faced with fraud. *“Enforcement takes up too much time, which companies are unwilling to spend. The company’s response depends on its tolerance to fraud and its appetite to deal with legal channels.”*

He acknowledges that many companies in India have tightened up their controls in recent years. Rather than whistleblowing or accidental discovery, most fraud is now detected by management review or because a manager becomes suspicious about a colleague’s behavior. *“However,”* says Mahajan, *“collusion between functions or with external parties means controls can be by passed which, in turn, results in an increase in fraud.”*

#### Most interesting fraud investigation

An individual, in his late 20s, committed a fraud worth over \$25 million.

He worked for a minerals company for more than four years, gaining the trust of senior management to such an extent that he was given responsibility for both hedging the price of minerals in the market and accounting for it in the back office. As a policy, the company did not seek to make a profit from hedging, but rather to guard against losses in a turbulent market.

The fraudster, deemed a very smart, hardworking, and honest employee, colluded with the company’s customers and passed discounts to them. He covered the discounts passed to customers by transferring profits from his illicit market speculation activities, accruing huge sums for himself as a “kick-back”.

Only when he was transferred to another function did his successor uncover the fraud. Although the company confronted the employee, they decided to take no legal action against him.

*“Indian companies are reluctant to seek legal redress and prefer separating the fraudsters (employees and external parties). Action taken by organizations greatly depends on their outlook and tolerance towards fraud as well as their appetite to deal with law enforcement and legal channels.”* says Mahajan.

The client engaged KPMG to investigate the extent of the fraud, the modus operandi, and the identities of those complicit in perpetrating it.

Rohit Mahajan heads the Forensic practice and is the national head for Investigation and Anti-Bribery and Corruption services in the Indian firm. With cross-industry experience, Rohit has worked on several high-profile cases involving the misappropriation of company assets and funds.

#### Contact Rohit Mahajan:

+91 223 989 6000

rohitmahajan@kpmg.com

# Size of the crime

Our analysis illustrates that the average identified and investigated total fraud loss in cases investigated by KPMG varies by geography. In Asia Pacific, the average loss was \$1.4 million; in the Americas, \$1.1 million; and in EMA, \$900,000 in 2011.



Further analysis reveals the following average total losses per fraud:

Sub region	Average total losses per fraud (millions of U.S. dollars)
Asia	1.5
Middle East	1.5
North America	1.2
Australia and New Zealand	1.1
Eastern Europe	1.0
Western Europe	0.9
Africa	0.9
South America	0.8
India	0.7

It is notable that the average total loss per fraud is substantial in some high-growth and BRIC economies as well as in some established economies. Effective controls to prevent and detect fraud in home and overseas markets are important not only to meet regulatory requirements but also to manage the substantial commercial losses associated with fraud and impropriety.

In the context of the individual transactions that make up the total fraud loss, the average transaction size in EMA was typically half that of Asia Pacific and the Americas. The lowest average transaction values were in India and Eastern Europe.

While it can be difficult and costly to recover losses, there has been a significant increase in attempts to mitigate losses between 2007 and 2011—up from 50 percent to 66 percent. This is possibly due to increased commercial pressures to recover funds.

There is, as might be anticipated, a direct correlation between the size of the crime and attempts to recover the loss. Companies attempted to recover losses in excess of \$25,000 nearly 60 percent of the time, rising to more than two thirds of the time where the loss exceeded \$50,000.

# Duration of fraud

Fraud now takes longer to detect—up from an average 2.9 years from inception to detection in 2007 to 3.4 years in the 2011 analysis.

In Asia, interestingly, the duration of fraud prior to detection is longest—on average five years—with 16 percent of frauds going undetected for 10 years or more. This is possibly because employees in Asia tend not to challenge their superiors or to rock the boat as much as in Western Europe or North America, where just 3 percent of fraud goes undetected for 10 years or more. In South America, Africa and the rest of Europe, none of the frauds investigated endured for more than 10 years before detection.

Fraud generally takes longer to detect in the emerged economies—North America averages 4.2 years, Australia 4.3, and Western Europe 3.7—compared with the high-growth economies. South America, for instance, averages 2.1 years.

For organizations where fraud endures over a number of years, questions need to be asked about the effectiveness of controls at detecting and preventing fraudulent activity and about the effectiveness of management oversight and responses to red flags.



“Although organizations plan for risk, they fail to appreciate just how likely and destructive the impact of a major fraud can be.”

says Mark Leishman

## View from Asia Pacific

### How does the global survey reflect regional findings?

The findings of the survey—notably in respect of the duration and size of fraud—are consistent with KPMG’s experiences in Asia Pacific. *“KPMG member firms often find that organizations move into Asia Pacific with the intention of tapping into larger markets or potentially cheaper sources of labor,”* says Mark Leishman, Investigation Services leader for KPMG’s Asia Pacific region. *“They do so, however, without truly understanding either the increased risks of fraud or the corruption they might face.”*

To overcome cultural and language barriers, there is, he observes, a tendency to staff subsidiaries with local people rather than with trusted and experienced employees from the home markets. This allows for gaps in controls and means that fraud can go undetected for prolonged periods, leading to high losses. *“The recovery rate in Asia Pacific is low. Often less than 5 percent of the losses incurred in Australia and New Zealand are retrieved,”* Leishman adds.

*“Although organizations plan for risk, they fail to appreciate just how likely and destructive the impact of a major fraud can be. To protect their businesses, fraud risk management needs to be sound, rigorously implemented, and able to anticipate and respond to the very worst case scenarios.”*

### Most interesting fraud investigation

A tip-off from a boutique retailer, revealing that it had received payments totaling several million dollars from the client’s accounts in recent months, alerted KPMG’s client to a potential fraud. The suspect was a long-serving senior finance employee, with an excessive lifestyle.

Using data analytics and other investigative techniques, KPMG identified the suspected misappropriation of more than \$40 million over six years and traced approximately 85 percent of it concealed in accounting records.

A review of online banking privileges identified poor segregation between transaction processing and approvals, false user profiles, and the deletion of large tranches of data. Key reconciliation processes were either nonexistent, overridden, or controlled by the suspect.

*“Within a few months of detection, KPMG had assisted the client in pursuing recovery of assets connected to the suspected fraud and with the police investigation. We assisted the client in collaborating with law enforcement and their legal representative to recover a significant amount of the stolen funds,”* says Leishman.

Mark Leishman joined KPMG in 2001 with 21 years’ experience in law enforcement. Today, Mark leads Investigation Services for KPMG’s Asia Pacific region from his Brisbane office in KPMG’s Australian firm. He previously headed up KPMG’s Forensic practices in the New Zealand and Korean firms.

Mark works across the wider Asia Pacific region, often on complex and sensitive investigations. He advises governments and provides investigation and fraud prevention support to organizations with offshore operations.

### Contact Mark Leishman:

+61 7 3233 9683

mleishman@kpmg.com.au

# Raising awareness

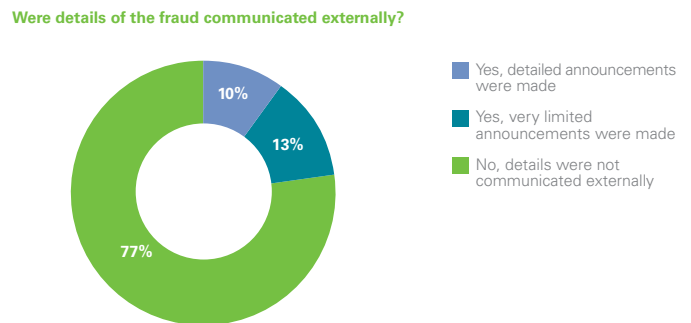
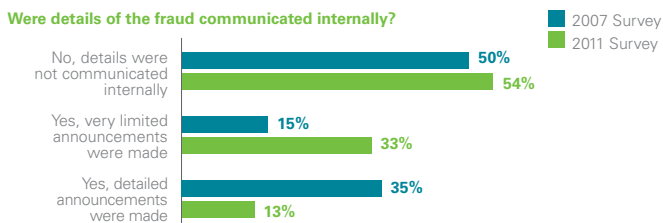
So how forthcoming are companies when it comes to telling others about the fraud and the penalties levied?

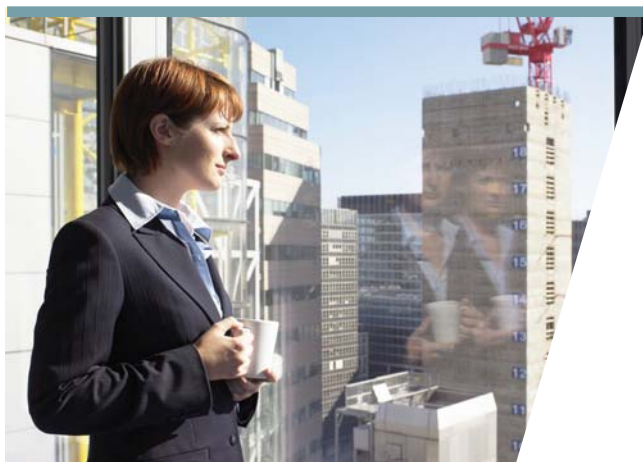


The 2011 survey data reveals a slight decrease in the internal disclosure of fraud, down from half of all cases in 2007 to 46 percent. Full disclosure of details fell from 35 percent in 2007 to 13 percent in 2011. India (88 percent of frauds not communicated) and Eastern Europe (72 percent) have least propensity to reveal details of fraud, while the most transparent countries are South Africa, Australia, and New Zealand. In 2011, they disclosed details in all but 36 percent of cases.

These figures suggest that companies may not take the opportunity to leverage learning points or to instill a culture of zero tolerance to fraud within the workplace. In many circumstances, follow-up procedures should include internal (and where appropriate external) communications to set the corporate tone on fraud and to deter its recurrence.

Companies tend not to make details of fraud publicly available, unless required by law, and/or when the loss is material to previously reported financial results. In the 2011 analysis, 77 percent of investigations did not reach the public domain.





However, reporting can be used to send a clear message to potential perpetrators that fraud will not be tolerated and increases the likelihood of recovery in the event of successful prosecution. Of course, where the financial loss is less significant than the potential damage to the corporate reputation, companies may choose not to report their suspicions to the police and will conduct their own internal investigations.

### Outcomes and responses

The outcomes of responses to incidents of fraud as a result of the analyzed KPMG investigations are as follows:\*

- Disciplinary action – taken in 40 percent of cases (54 percent in the Americas, compared with 23 percent in Asia Pacific);
- Enforcement action (includes regulatory, legal and police) – in 45 percent of cases (the lowest instances were in EMA at 40 percent);
- Civil recovery – 23 percent of cases;
- Resignation/voluntary retirement – 17 percent of cases (25 percent in Asia Pacific);
- Settled out of court – 6 percent of cases;
- Took no action or sanction – 3 percent of cases (all but one was in EMA).

By geography, the survey reveals the most frequent outcomes:

#### North America

Enforcement action was taken in 63 percent of cases, disciplinary action in 66 percent of cases and civil recovery in 37 percent of cases. This pattern reflects the strong regulatory and enforcement framework in North America.

\* Percentages add up to more than 100 percent due to multiple outcomes/entity responses in many cases.

#### South America

The likelihood of enforcement or disciplinary action in South America was almost half that in North America (36 percent for each).

#### Asia

Enforcement action was taken in 40 percent of cases. The region had the highest incidences of resignation/voluntary retirement—28 percent—than anywhere else in the world.

#### Africa

Enforcement action (including police and legal action) was taken in 65 percent of cases, with disciplinary action also high at 51 percent.

#### Eastern Europe

Disciplinary action is the most common recourse of fraud in Eastern Europe. This was taken in 33 percent of cases and resignation/voluntary retirement in 24 percent. However, enforcement action was taken in just 17 percent of cases and civil recovery in 2 percent, reflecting unique legal, regulatory, and cultural frameworks in these jurisdictions.

#### India

Enforcement action was taken in one-quarter of cases. Similarly, disciplinary action occurred in 25 percent of cases and resignation/voluntary retirement in 19 percent.

#### Middle East

Enforcement action was taken in 57 percent of cases, civil recovery in 43 percent, and disciplinary action in 29 percent.

In this region, resignation/voluntary retirement was not taken in any of the cases investigated.

#### Western Europe

In 42 percent of cases, enforcement was taken. Disciplinary action was taken in 41 percent, civil recovery in 26 percent, and resignation/voluntary retirement in 13 percent of cases.

“Even in a well-regulated market and with a good audit function, massive frauds can go undetected for a number of years.”

says Déan Friedman

## View from South Africa

### How does the global survey reflect regional findings?

*“The profile in South Africa is largely consistent with the findings of the global survey. However, unique conditions also prevail,”* says KPMG Forensic Partner Déan Friedman. *“What can be described as economic hijacking is becoming increasingly prevalent and impedes investor confidence.”*

It manifests in three distinct ways:

#### Company hijacking

Company details, including the names and details of officers and directors of the company, are changed without authority. This enables fraudsters to obtain, for instance, bank loans in the company’s name. *“They then channel the proceeds to themselves via an impaired loan account. Unpaid debts can accumulate, leaving the bank with an impaired loan and the company in debt and unable to obtain working capital,”* explains Friedman.

#### Wholesale dispossession of company assets

Fraudsters materially or completely strip companies of their assets and/or their means to generate income. These rare but highly damaging instances leave creditors and shareholders with little prospect of recovering their losses.

#### Hijacking of state-allocated rights

In some industries, notably resources, the South African government allocates rights to companies to engage in certain activities. It may take several years of ongoing capital injection before economic return is achieved. However, security of tenure is at risk. More and more allegations are surfacing about fraudulent applications and exploitation of relationships, which see rights diverted elsewhere.

#### Most interesting fraud investigation

KPMG Forensic was appointed to investigate the largest corporate fraud in South Africa’s history. The case concerned two mining companies, both largely controlled by the same directors and officers. Some directors were also significant stakeholders in each.

When funding pressures hit one company, the assets of the other were used to secure borrowings by short-selling shares to the market. However, the prevailing bull market put increased pressure on the company resources used to secure these long-dated structures. Over time, the directors and officers of the company disposed of all of the assets of one company to satisfy the funding needs of the other. Some directors also benefitted from the disposals.

These transactions led to a five-year investigation of claims against third parties, directors, and company officers. It involved analysis of accounting practices, criminal conduct, and regulatory abuses. The investigation revealed significant skill and cynicism in simulating transactions and financial structures to disguise the existence and disposition of the dispossessed assets in the companies’ financial statements. The requirements of the stock exchange and the audit function’s own procedures meant that the issues were eventually made public. By this time, however, significant assets were lost irretrievably.

*“Even in a well-regulated market and with a good audit function, massive frauds can go undetected for a number of years,”* says Déan Friedman. *“By instigating detailed investigations before committing funds, stakeholders can be protected from significant loss. Investigations can be proactive in purpose, by articulating evidence of activities and positions that may lead to future loss. This is in addition to the more traditional purpose of redress normally associated with reactive investigations.”*

Déan Friedman is the partner responsible for Investigations, Corporate Intelligence and Asset Preservation approaches in KPMG’s South African firm. His experience crosses several industry sectors and geographies. He formerly prosecuted fraud and other commercial crime charges on behalf of the state in South Africa’s regional and high courts.

#### Contact Déan Friedman:

+27 (11) 647 8033

dean.friedman@kpmg.co.za

# Fraud is up; defenses are down

Our analysis indicates that fraud and misstatement of results continue to be growing problems for companies at a time when budgets are stretched. Defenses, however, seem to be less effective than they used to be.



In summary, the general characteristics of the fraudster appear to be changing only moderately. We see the middle-aged member of middle to senior management still being the subject of many of our fraud investigations. There is a slight trend toward the individual being more tenured at the company. More interesting is how the failure to initially respond to red flags and lapses in internal controls were an increasing contributor to enabling the fraud to occur. Also, the impact of the economic crisis seemed to have resulted in an increasing number of companies seeking to recover their fraud losses, in hopes of minimizing the financial consequences to the organization.

With increased economic pressures on individuals, failure to identify or address red flags and the lengthening time lapse between fraud inception and detection, the likelihood is that frauds, currently undetected, will emerge in greater numbers in the next two to three years.

For companies, the challenge is how to see through the “ordinary” disguise of the fraudster; how to close gaps in the corporate armor; how to enhance fraud prevention and detection efforts; and how to respond more often, more appropriately, and more rapidly to red flags.

# Red flags not to be missed

Your “average” fraudster, based on our analysis, is someone who has worked in an organization for many years, is considered trustworthy, and has a more senior position. But which key areas of your business may be most susceptible to fraud? And what behaviors among employees should not be ignored?

Here are just some of the red flags to look out for:

Does this describe an area of your business?	Yes	No		Yes	No
There are difficult relationships and a possible lack of trust between the business and the internal/external auditor.			There are multiple banking arrangements rather than one clear provider—a possible attempt to reduce transparency over the business’ finances.		
Excessive secrecy about a function, its operations, and its financial results. When questions are asked, answers and supporting information are often stalled or withheld.			A division or department of the business is perceived as complex or unusually profitable, thereby diverts the attention of management and the audit functions.		
Some practices within a function do not appear straight-forward, and may even be illegal or unethical.			Where matters of financial judgment/accounting treatment are involved, the business consistently pushes the limits/boundaries.		
There is excessive pressure on employees to tamper with results to meet analysts’ high expectations for the business.			High staff turnover within a function. Employees may be more likely to commit fraud in a business with low morale and inconsistent oversight.		
Elsewhere in the industry, companies are struggling and sales and/or profits are declining. Your business appears to buck the trend.			Complex/unusual payment methods, agreements between the business and certain suppliers/customers, may be set up in a deliberately opaque manner to hide their true nature.		
Increases in profitability fail to lead to increased cash flows.			A remote operation not effectively monitored by the head office.		
Senior managers receive large bonuses linked to meeting targets.					

As we have seen, there are certain characteristics that typify a fraudster. Employee awareness of other behaviors can help businesses identify frauds earlier. Be alert to the following employee behavioral red flags:

Do you work with someone who displays these behaviors?	Yes	No		Yes	No
Refuses or does not seek promotion and gives no reasonable explanation.			Volatile and melodramatic, arrogant, confrontational, threatening, or aggressive when challenged.		
Rarely takes holidays.			Is suspected to have over-extended personal finances.		
Does not or will not produce records/information voluntarily or on request.			The level of performance or skill demonstrated by new employees does not reflect past experience detailed on CVs.		
Unreliable and prone to mistakes and poor performance.			Cuts corners and/or bends rules.		
Tends to shift blame and responsibility for errors.			Seems unhappy at work and is poorly motivated.		
Surrounded by “favorites” or people who do not challenge them.			Accepts hospitality that is excessive or contrary to corporate rules.		
Persistent rumors/indications of personal bad habits/addictions/vices.			Seems stressed and under pressure.		
Bullies or intimidates colleagues.			Has opportunities to manipulate personal pay and reward.		
Vendors/suppliers will only deal with this individual.			Self-interested and concerned with own agenda.		
Lifestyle seems excessive for income.			Micromanages some employees; keeps others at arm’s length.		

# Further guidance on how to keep your business safe

KPMG's analysis of the fraudster is just part of our firms' forensic support for companies and public-sector entities. We can help you to build effective anti-fraud programs and implement fraud prevention and detection strategies, as well as respond to instances of fraud and misconduct.



Three further KPMG publications explore how to deal with the threat of fraud in your organization.

## **MANAGING THE RISK OF FRAUD AND MISCONDUCT: MEETING THE CHALLENGES OF A GLOBAL, REGULATED, AND DIGITAL ENVIRONMENT** (published by McGraw-Hill)

This book, co-authored by KPMG partners **Richard H. Girgenti** and **Timothy P. Hedley**, with the collaboration of many Forensic partners and professionals, is designed to help organizations navigate the risks of fraud and misconduct that can jeopardize their bottom lines and business reputations.

Published by McGraw-Hill in March 2011, the book is a guide to help business leaders set their organizations on the right path, whether evaluating a global acquisition in an atmosphere of increased multinational enforcement of anti-corruption laws or simply trying to implement an anti-fraud program throughout the enterprise.

The book also discusses strategies to help organizations tackle challenges that range from the financial reporting fraud scandals of a decade ago, to the implications of the more recent massive Madoff and Stanford Ponzi schemes, or the investigations of insider trading in the hedge fund industry. While trying to keep one eye on fast-paced economic and regulatory changes, business leaders should also be attentive to risks of fraud and misconduct that can jeopardize their success.

## **FRAUD RISK MANAGEMENT: DEVELOPING A STRATEGY FOR PREVENTION, DETECTION, AND RESPONSE**

This white paper provides an overview of fraud risk management fundamentals, identifies key regulatory mandates from around the world, and puts the spotlight on practices that organizations generally find to be effective.

As you consider the risks of fraud at home and abroad, and the effectiveness of the controls you rely on to mitigate those risks, this document provides relevant insight.

To view the document online, go to:

<http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Fraud-Risk-Management-O-200610.pdf>

## **CROSS-BORDER INVESTIGATIONS: EFFECTIVELY MEETING THE CHALLENGE**

This white paper shares the findings of a KPMG International survey completed in conjunction with research firm Penn, Schoen and Berland Associates, Inc.

The survey considers the principal challenges faced by multinational businesses in diverse industries around the world in responding to cross-border investigations, and summarizes the opinions of senior executives interviewed as part of the survey. The paper also provides insights into possible responses to those challenges.

We use those insights to consider how companies can derive best value for their current or pending investment in cross-border investigations, regardless of whether those are conducted in-house or undertaken with a third party.

To view the document online, go to:

<http://www.kpmg.com/Ca/en/IssuesAndInsights/ArticlesPublications/Documents/Cross-Border%20Investigations.pdf>

At the back of this document, find the contact details of a number of KPMG Forensic leaders in some of our accredited practices across the globe who can guide you in your own anti-fraud activities.



## Contacts

### **Richard Girgenti**

**Americas Forensic Service Line Leader**

**T:** +1 212 872 6953

**E:** rgirgenti@kpmg.com

### **Phillip D. Ostwalt**

**Americas Investigations Network Leader**

**T:** +1 404 222 3327

**E:** postwalt@kpmg.com

### **Ian Colebourne**

**EMA Forensic Service Line Leader**

**T:** +7 495 937 2524 ext:12203

**E:** iancolebourne@kpmg.ru

### **Richard Powell**

**EMA Investigations Network Leader**

**T:** +44 161 246 4044

**E:** richardfa.powell@kpmg.co.uk

### **Grant Jamieson**

**AsPac Forensic Service Line Leader**

**T:** +85 22 140 2804

**E:** grant.jamieson@kpmg.com

### **Mark Leishman**

**AsPac Investigations Network Leader**

**T:** +61 7 3233 9683

**E:** mleishman@kpmg.com.au

### **Jack de Raad**

**ELLP Forensic Service Line Leader**

**T:** +31 20 656 7774

**E:** deraad.jack@kpmg.nl

### **Gerrie Lenting**

**The Netherlands, Forensic Service Line Partner**

**T:** +31 20 656 4632

**E:** lenting.gerrie@kpmg.nl

#### **Acknowledgements**

KPMG's contributors to this publication include:

Dana G McFerran, Will Hanley III, Jackie Gillson, James D McAuley, John Ederer, Owen Hawkes, Gerrie Lenting, Barbara Legg, David Watterson, Kerstin Drossard, Jane Honeyford and Paul Milman.

**We would also like to thank all the individuals who contributed to the analysis.**