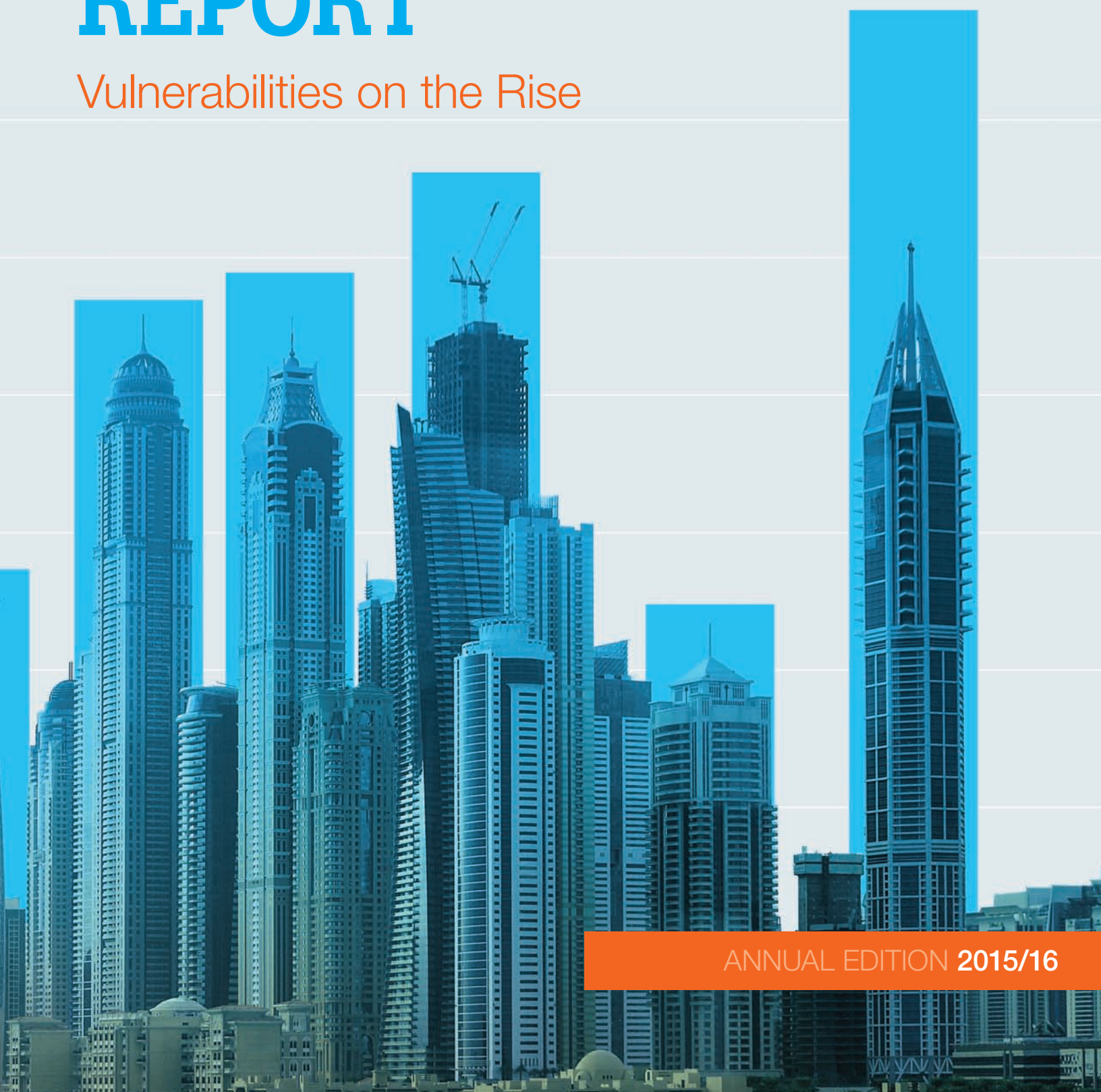
Kroll

GLOBAL FRAUD REPORT

Vulnerabilities on the Rise



ANNUAL EDITION **2015/16**

ABOUT THE RESEARCH

The Annual Global Fraud Survey, commissioned by Kroll and carried out by the Economist Intelligence Unit, polled 768 senior executives worldwide from a broad range of industries and functions from January through March of 2015. Where Economist Intelligence Unit analysis has been quoted in this report, it has been headlined as such. Kroll also undertook its own analysis of the results. As in previous years, these represented a wide range of industries, including notable participation from Financial Services and Professional Services as well as Retail, Wholesale and Distribution; Technology, Media and Telecommunications; Healthcare, Pharmaceuticals and Biotechnology; Transportation, Leisure and Tourism; Consumer Goods; Construction, Engineering and Infrastructure; Natural Resources; and Manufacturing. Respondents were senior, with 50% at the C-suite level. Over half (51%) of participants represent companies with annual revenues of over $500 million. Respondents this year included 29% from Europe, 25% from North America, 24% from the Asia-Pacific region, 10% from Latin America and 12% from the Middle East/Africa. This report brings together these survey results with the experience and expertise of Kroll and a selection of its affiliates. It includes content written by the Economist Intelligence Unit and other third parties. Kroll would like to thank the Economist Intelligence Unit, Dr. Paul Kielstra and all the authors for their contributions in producing this report. Values throughout the report are U.S. dollars.

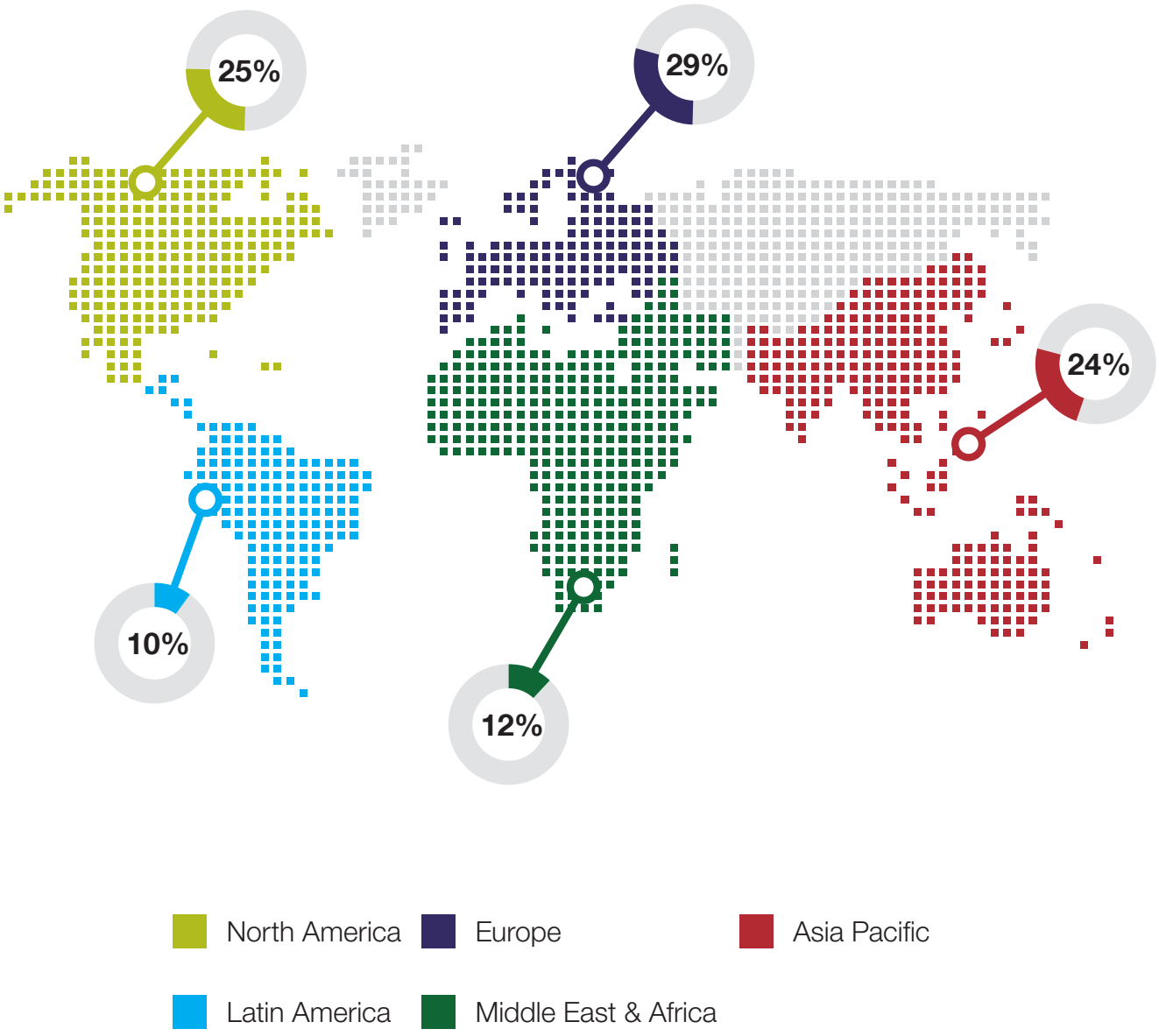

25%
29%
24%
10%
12%
North America
Europe
Asia Pacific
Latin America
Middle East & Africa

Table of Contents

OVERVIEW

NORTH AMERICA OVERVIEW

SOUTH AMERICA OVERVIEW

ASIA PACIFIC OVERVIEW

EMEA OVERVIEW

ECONOMIST INTELLIGENCE UNIT REPORT CARDS

SUMMARY

FRAUD ON THE RISE

For the eighth year running, The Economist Intelligence Unit, commissioned by Kroll, surveyed senior executives from around the world operating in a wide variety of sectors and functions in order to assess the current fraud environment.

The overall observation is that fraud has continued to increase, with three quarters (75%) of companies reporting they have fallen victim to a fraud incident within the past year, an increase of 14 percentage points from just three years ago. The number of businesses suffering a financial loss as a result of fraud has also increased, from 64% in the previous survey period to 69% this year.

The report reveals some key trends:

Firms feeling more vulnerable to fraud

Theft of physical assets was the most common fraud experienced in the past year, cited by 22% of respondents. Vendor, supplier or procurement fraud (17%) and information theft (15%) are the next two most frequent types of fraud experienced.

But the reported incidents just tell part of the story, with the vast majority of respondents (80%) believing their organizations have become more vulnerable to fraud in the past year. One of the areas identified by executives as being of particular concern is information theft. More than half of executives (51%) believe they are highly or moderately vulnerable to information theft risks such as cyber incidents.

This increased awareness level has led to growth in the number of companies proactively looking after their information security posture. Two-thirds (67%) of companies report that they regularly conduct data and IT infrastructure assessments, and a majority now report that they have an up-to-date information security incident response plan (60%) and have tested it in the past six months (59%), both representing an increase from the previous survey.

The globalization of business increases fraud risk

In a global marketplace where many international businesses have thousands of companies in their supply chain, risks become more difficult to identify and keep under control. Companies feel particularly at risk of threats such as vendor, supplier or procurement fraud, with half of respondents (49%) feeling highly or moderately vulnerable to it.

Logically, larger companies that are more likely to have bigger supply chains felt significantly more vulnerable to this type of fraud, with 20% of businesses with a turnover of more than $500 million considering themselves highly vulnerable to it, compared to just 14% of firms with a turnover of less than $500 million.

CHART 1

COMPANIES AFFECTED BY FRAUD AND VULNERABLE TO IT

TYPES OF FRAUD	PERCENTAGE OF COMPANIES AFFECTED BY THIS IN THE PAST 12 MONTHS	PERCENTAGE OF COMPANIES DESCRIBING THEMSELVES AS HIGHLY OR MODERATELY VULNERABLE TO THIS
Theft of physical assets	22%	62%
Vendor, supplier or procurement fraud	17%	49%
Information theft	15%	51%
Management conflict of interest	12%	36%
Regulatory or compliance breach	12%	40%
Corruption and bribery	11%	40%
Internal financial fraud	9%	43%
Misappropriation of company funds	7%	40%
Money laundering	4%	34%
IP theft	4%	37%
Market collusion	2%	26%

Some 40% of respondents felt highly or moderately vulnerable to corruption and bribery, another type of fraud that increases in propensity as companies expand geographically into new territories.

Indeed, in the past year, 72% of companies were dissuaded from operating in a particular country or region because of the heightened exposure it would bring to fraud. Latin America (cited by 27% of all respondents) was the region which saw most businesses turn away, but the other perennial region of concern, Africa, was not far behind (22%).

Many executives see moving into new geographic markets as risky business. One in eight (13%) of those who say their company's exposure to fraud has increased claim entry into new, riskier markets is a reason for this. One in five (20%) say a greater level of outsourcing and offshoring have contributed to their increased fraud exposure.

CHART 2

TOP THREE REGIONS COMPANIES ARE AVOIDING DUE TO HEIGHTENED FRAUD EXPOSURE

REGION	PERCENTAGE OF COMPANIES THAT HAVE BEEN DISSUADED FROM OPERATING HERE BECAUSE OF THE HEIGHTENED EXPOSURE IT WOULD BRING TO FRAUD
Latin America	27%
Africa	22%
Central & Eastern Europe	14%

The threat from within is on the rise

The findings reveal the biggest fraud threat to companies comes from within. Of those companies that experienced fraud where the perpetrator was known, four in five (81%) suffered at the hands of at least one insider, up from 72% in the previous survey.

More than one in three victims (36%) experienced fraud at the hands of a member of their own senior or middle management, 45% at the hands of a junior employee, and for 23%, the fraud resulted from the conduct of an agent or intermediary.

Currently, much media attention is focused on external cyber threats to companies, but the findings of the report tell a different story. Of those companies that have fallen victim to information loss, theft or attack over the past 12 months, the most common cause was employee malfeasance, involved in 45% of cases, with vendor/supplier malfeasance involved in 29% of cases. By comparison, only a small minority of cases involved an attack by an external hacker on the company itself (2%) or on a vendor/supplier (7%).

With employees constituting such a high risk, it is not surprising that executives responding to the survey believe that high staff turnover is the main driver of increased exposure to fraud, with one in three (33%) citing it as being a problem. This is more than twice as many who named the next highest driver of vulnerability to fraud, greater outsourcing (16%).

In an environment where insiders are the source of the problem, other employees who observe or become aware of what the fraudsters are doing are the company's strongest defense. In the past year, a whistleblower was at least partially responsible for exposing 41% of cases

CHART 3

TOP FIVE DRIVERS OF INCREASED FRAUD EXPOSURE

DRIVER OF INCREASED FRAUD RISK	PERCENTAGE OF EXECUTIVES WHO BELIEVE THIS HAS INCREASED THEIR COMPANY'S EXPOSURE TO FRAUD OVER THE PAST 12 MONTHS
High staff turnover	33%
Increased outsourcing & offshoring	16%
Entry to new, riskier markets	13%
Complexity of products or services sold	11%
Increased collaboration between firms (e.g., joint ventures, partnerships)	10%

of fraud that were uncovered. Employee-discovered and reported fraud is well ahead of the next two sources of discovery, external (31%) or internal (25%) audits.

The findings show that anti-fraud efforts can have an effect on the threat from within. Of those firms hit by fraud where the perpetrator was known, just 20% of those with management controls in place suffered at the hands of a senior or middle manager compared to 31% of firms without such controls.

CHART 4

TOP THREE METHODS OF EXPOSING FRAUD

METHOD OF DISCOVERY	PERCENTAGE OF UNCOVERED FRAUDS THAT WERE EXPOSED VIA THIS METHOD
Whistleblower	41%
External audit	31%
Internal audit	25%

CHART 5

PERPETRATORS OF KNOWN FRAUDS

GROUP	PERCENTAGE OF FIRMS HIT BY FRAUD WHERE SOMEONE IN THIS GROUP WAS A KEY PERPETRATOR
Junior employees	45%
Vendors/Suppliers	18%
Agents and/or Intermediaries	23%
Senior or middle management	36%
JV partners	8%
Regulators	7%
Customers	5%
Government officials	3%
Other	3%

Conclusion

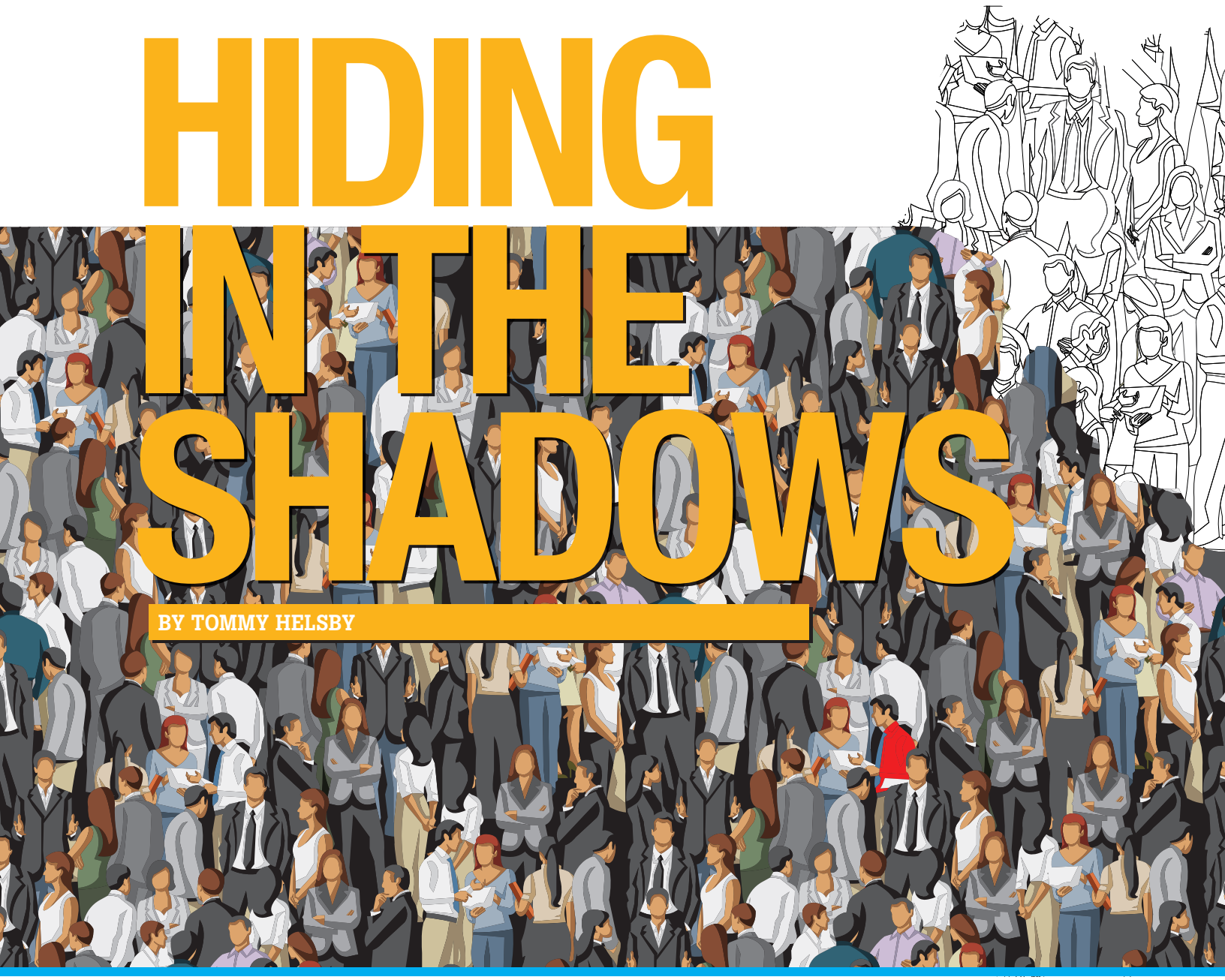
From widespread corruption allegations in FIFA to laundering Russian mafia money in high-end London real estate, fraud is never far from the headlines. What our report and our day-to-day experience tell us is that despite companies making greater and more sophisticated efforts to combat fraud, it remains a serious business threat that cannot be completely eliminated. The adverse impacts of such incidents cannot be underestimated.

Fraud is virulent, and perpetrators adapt their methods on an ongoing basis. As one barrier is put up, fraudsters will seek and find an alternative weakness to exploit. This type of persistence and stealth is especially evident in the creative ways digital networks are constantly being attacked and often penetrated.

In the face of such motivated adversaries, businesses must implement procedures that can help them identify, mitigate and manage fraud risks. There is no absolute or perfect solution, and the techniques employed by fraudsters evolve and are ever-changing. As a result, energy and effort has to be focused not only on prevention, but also on response in the event that such fraudulent efforts are able to circumvent processes and other preventive measures. Being positioned to implement a rapid and decisive response is equally as critical to mitigating such risks. Fraud is not going away and continues to be on the rise, but the well-prepared business can do much to stay one step ahead and be positioned to eliminate or mitigate it.

HIDING IN THE SHADOWS

BY TOMMY HELSBY



There is a curious contradiction in this year's Global Fraud Survey statistics: the proportion of respondents reporting at least one fraud in their company in the past year has risen to its highest level in the report's eight-year history at 75%, but every separate category of fraud has decreased.

A contradiction in the facts always hides something interesting, as investigators have known since Sherlock Holmes mused about the dog that didn't bark in the night. Is there a new category of fraud that we have missed? Not likely: every kind of commercial wrongdoing will fall somewhere on our list. And we did not make a mistake adding the numbers—our forensic accountants checked!

I think the answer lies in the nature of fraud statistics—and that answer is interesting and important. Some fraud surveys claim to have hard numbers: an annual total number of cases and a dollar amount for the losses incurred. But this can only record publicly reported cases, and in our experience, this is a small proportion of the total. Those that are reported typically extend over a number of years, making annual trends meaningless. Lastly, no survey can ever measure unproved and undiscovered fraud, probably the largest categories of all, making loss statistics questionable.

Our survey measures perceptions of fraud. We survey senior executives from a broad range of industries in every part of the world about their experience and awareness of fraud. They may not always have detailed knowledge of the incidence and quantum of frauds—in our experience, specific knowledge will be quite tightly held. But as part of the senior management of their organizations, they have an insight into the policies of their companies and what drives them, and so have a very good sense of where risks and opportunities lie. What is very clear is that fraud has risen inexorably up the corporate priority list.

Fraud, corruption and regulatory violations now fill more space in the business press than mergers and acquisitions, with "massive fines" replacing "massive fees" in the related headlines. It is increasingly recognised that boards have a duty to report to shareholders on their response to fraud and regulatory exposure along with other risks. So it is on the agenda and in people's minds, and the headline result in our Survey reflects this clearly. The apparent decrease in each of the individual categories probably reflects a lack of specific knowledge of the details of the frauds, and so the allocation by type may in many cases involve some guesswork on the part of the respondent.

Given that we are looking at perceptions, these guesses suggest another interesting insight. Respondents' top concern is, as always, theft of physical assets, followed by vendor fraud and then information theft.

Each of these looks like threats from outside the company, although a little thought will tell you that the threat is probably greater from employees, either directly or in collusion with outsiders. Concern about conflict of interest, regulatory breaches, corruption, internal fraud and misappropriation of funds—all clearly insider issues—are significantly lower.

It is, of course, far more comforting to think of the threat coming from the outside rather than lurking among colleagues within the company. This is most evident in attitudes to hacking: company executives (encouraged by the media) worry more about North Koreans than what is happening in the next cubicle despite the evidence—and our practical experience—that most breaches have an inside dimension. Furthermore, there is a limit to what you can do about threats from North Korea, but there are plenty of effective measures to tighten internal systems and improve employee behavior.

When a fraud is discovered, there is generally a degree of delicacy about conducting internal inquiries. Some is justified: you don't want to tip off those involved until you are ready. But there is often a concern in senior management about the impact of an internal investigation on morale: "We don't want to be seen conducting a witch-hunt." In our experience, people on the ground often know far more than senior management thinks, and the lack of a properly handled investigation can seem at best as indifference and at worst as if the blame may be spread too widely.

If an internal investigation is required, it must be properly handled, and in an increasingly multinational corporate environment, that requires an understanding of cultural, business and legal nuances in different countries. The arrival of the man from head office, with his newly issued passport, wondering why the office is closed on a Friday, is not likely to produce useful results in the Gulf, and the demand for a full email review in Germany will (hopefully) result in a swift education in data privacy laws. The articles in this Global Fraud Report give some helpful insights into the types of issues that we have encountered around the world and in the newer frontier of cyberspace. As I have said many times, most of what we do is common sense, but it's based on uncommon experience.

Tommy Helsby is Chairman of Kroll, based in London. Since joining Kroll in 1981, Tommy has helped found and develop the firm's core due diligence business and managed many of the corporate contest projects for which Kroll became well known in the 1980s. Tommy plays a strategic role both for the firm and for many of its major clients in complex transactions and disputes. He has a particular interest in emerging markets, especially Russia and India.

The prevalence of fraud

We polled 768 senior executives from a broad range of industries worldwide this year—and the results yielded some surprising insights. The overall picture is that fraud has continued to increase, leaving businesses feeling more vulnerable and at risk than ever before.

The panels on the map summarize:

- The percentage of respondents per region or country suffering at least one fraud in the last 12 months
- The top four areas and drivers of most frequent loss in each region or country

EUROPE

74 % Experienced fraud

27 % Theft of physical assets or stock

18 % Vendor/supplier/procurement fraud

16 % Information theft, loss or attack

15 % Regulatory or compliance breach

CANADA

65 % Experienced fraud

26 % Theft of physical assets or stock

23 % Vendor/supplier/procurement fraud

19 % Management conflict of interest

16 % Information theft, loss or attack

UNITED STATES

75 % Experienced fraud

22 % Theft of physical assets or stock

19 % Vendor/supplier/procurement fraud

17 % Information theft, loss or attack

15 % Regulatory or compliance breach

MEXICO

80 % Experienced fraud

23 % Theft of physical assets or stock

23 % Vendor/supplier/procurement fraud

17 % Information theft, loss or attack

10 % Misappropriation of company funds

COLOMBIA

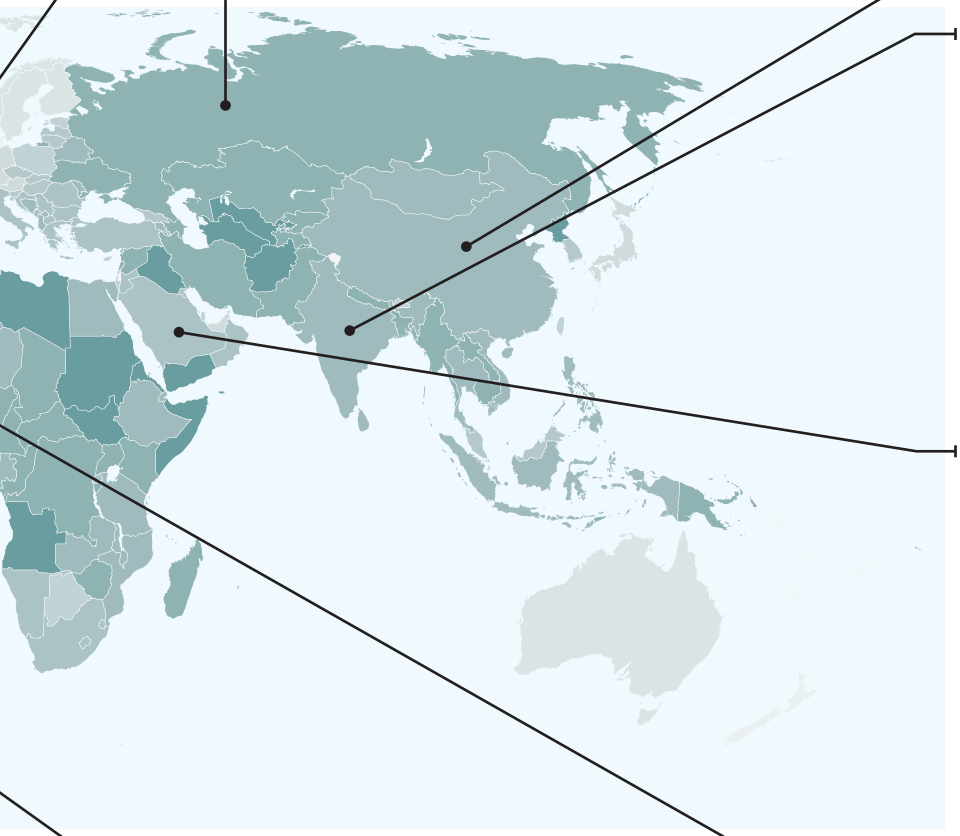
83 % Experienced fraud

27 % Information theft, loss or attack

23 % Management conflict of interest

17 % Theft of physical assets or stock

13 % Vendors/supplier/procurement fraud



RUSSIA

73 % Experienced fraud

20 % Theft of physical assets or stock

20 % Corruption and bribery

17 % Misappropriation of company funds

13 % Vendor/supplier/procurement fraud

CHINA

73 % Experienced fraud

23 % Theft of physical assets or stock

18 % Corruption and bribery

16 % Information theft, loss or attack

13 % Vendor/supplier/procurement fraud

INDIA

80 % Experienced fraud

25 % Corruption and bribery

23 % Vendor/supplier/procurement fraud

20 % Regulatory or compliance breach

18 % Theft of physical assets or stock

THE GULF STATES

63 % Experienced fraud

18 % Vendor/supplier/procurement fraud

15 % Misappropriation of company funds

13 % Theft of physical assets or stock

13 % Management conflict of interest

BRAZIL

77 % Experienced fraud

23 % Internal financial fraud

17 % Theft of physical assets

17 % Vendor/supplier/procurement fraud

10 % Information theft, loss or attack

SUB-SAHARAN AFRICA

84 % Experienced fraud

24 % Theft of physical assets or stock

22 % Vendor/supplier/procurement fraud

14 % Misappropriation of company funds

14 % Corruption and bribery

United States overview

Contrary to the common perception that the United States is a low-fraud location, it is a country with a fraud problem just like any other with our survey revealing figures very close to the global average. The overall prevalence (75% of companies affected by at least one fraud in the past year) was the same as the survey mean and the average loss (0.9% of revenues) slightly higher than that for all respondents (0.8%). Similarly, the incidence of most frauds was within one or two percent of the survey average.

The survey also shows that the country has a substantial problem with insider fraud: where a fraud had occurred in the past year and the perpetrator was known, 40% of American respondents said that a senior or middle manager had been a major player in at least one such crime, noticeably above the global average of 36%.

Where the United States' figures stand out is the prevalence of fraud perpetrated by business counterparties outside the firm. This manifests itself in a variety of ways. Vendor fraud affected 19% of American companies in the last year, the country's second most common fraud. More striking, in cases of information theft, vendor or supplier malfeasance played a major role 46% of the time—one of the highest figures of any country in this analysis. In addition, a joint venture partner was a leading player in 13% of cases of U.S. companies suffering from fraud with a known perpetrator in the past year—the highest figure for any country reported on.

UNITED STATES REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	75%	66%
LOSS Average percentage of revenue lost to fraud	0.9%	1.2%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Theft of physical assets or stock **(22%)** ■ Vendor, supplier or procurement fraud **(19%)** ■ Information theft, loss or attack **(17%)**	■ Management conflict of interest **(21%)** ■ Information theft, loss or attack **(20%)** ■ Theft of physical assets or stock **(20%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**79%**	**81%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(34%)** ■ Increased outsourcing and offshoring **(15%)** ■ Increased collaboration between firms **(15%)**	■ IT complexity **(44%)**

Medical marijuana partnership risks: Not just blowing smoke

By Jeffrey Cramer, Senior Managing Director

Public sentiment regarding the use of marijuana has shifted dramatically over the past several years. As of April 2015, medical marijuana is legal in 25 U.S. states and the District of Columbia. Additionally, nine states have pending legislation, and 12 states have legalized the limited use of low-THC marijuana for medical purposes. Recreational use is legal in four states. Despite the fact this "black" market has become "white" in many states, those involved in the industry still find themselves at significant risk of criminal prosecution and reputational ruin.

The sale, possession, production and distribution of medical marijuana remain illegal under federal law. States that have legalized marijuana have seen hundreds of raids on dispensaries, particularly in Colorado and California, many of which were operating in compliance with state law. The states that have legalized marijuana have only been able to do so because of federal guidance urging prosecutors to refrain from targeting state-legal marijuana operations. Some of this guidance explicitly discusses the possibility for fraud and notes the obligation for those involved in the industry to undertake appropriate due diligence. This level of due diligence must be more than just a perfunctory check to see if there are any criminal activities in a local jurisdiction.

The call for appropriate due diligence is grounded in the fact that the industry has been rife with fraud. In 2012, a registered caregiver under the Rhode Island Medical Marijuana Program was sentenced to prison for illegally cultivating marijuana plants. In May 2013, a grower registered under the Oregon Medical Marijuana Program was sentenced to 15 years in prison after a jury found he was using his license to "create the appearance" that he was complying with the Oregon law while actually selling most of the marijuana illegally. In May 2014, federal prosecutors in Denver levied international money laundering charges against a local attorney and three others, claiming that the group had wired and laundered hundreds of thousands of dollars from Colombia to buy a Denver grow house.

As the limited history of the industry has shown, not all growers and dispensary owners adhere to the ethical standards required by the states, and fraud is endemic. In February 2015, in the first case of its kind in California, prosecutors alleged organized crime was running a chain of northern California medical marijuana clinics. Federal agents arrested the alleged owner of the chain and accused him of money laundering and generating millions of dollars for the Ukrainian mob.

With this as a backdrop, more sophisticated investor groups are looking at medical marijuana licenses as a potential revenue stream. Private equity funds, international consortiums, hedge funds and the like are looking to secure these licenses to partner with state governments. Because investors behind the license bidders can come and go, the risk for states and applicants will be an evolving problem. State entities will be under the microscope by cities, media and other stakeholders to ensure they are partnering with reputable investors. It will be important to know that the money behind these groups is not tainted. Money laundering will be a real concern. In our experience, the source of funds and the backgrounds of the primary individuals are better learned before a contract is signed. The legal and public scrutiny afterwards can cause tremendous problems.

Probity and due diligence are critical to the sustainability of this market sector. States issuing licenses, private equity funds investing in the businesses, insurance companies, and financial institutions accepting funds are among those who must take appropriate care to ensure these businesses are operating aboveboard and to the highest standards of integrity.

In part, organized crime has found a place in this industry because of the conflict between federal and state laws and, thus, the reluctance of banks to provide financial services to medical marijuana growers and dispensers. To banks, the pre-eminence of federal law has been a powerful deterrent to allowing pot businesses to set up accounts. The Financial Crimes Enforcement Network (FinCEN) issued guidance in February 2014 that tacitly acknowledged the legality of banking marijuana businesses.

The guidelines were widely touted as a way to get money into the banking system where it could be more easily tracked and less likely to be controlled by organized crime. As part of this guidance, FinCEN called for due diligence by financial institutions in monitoring their marijuana customers. This diligence includes reviewing the accuracy of information disclosed in their state license applications and understanding their "normal and expected activity." Even so, in March 2015, federal prosecutors in Washington brought drug conspiracy and related charges against several family members. The defendants were convicted of growing marijuana but acquitted of the remaining four counts. The defendants argued they were growing the marijuana for their own medical use.

Despite the federal guidelines, banks have been reluctant to take on the risks associated with the industry. For many growers and distributors, finding a bank to provide services is still a "pipe dream" according to a 2014 article in the Wall Street Journal. Because financial transactions of a marijuana business are illegal under federal law, banks must still file suspicious activity reports (SARs) when a new pot business opens or closes an account or when such businesses exhibit activities that violate the guidelines.

These SARs provide some insight into the rapid growth of this industry. In August 2014, FinCEN director Jennifer Shasky Calvery stated almost half of the SARs (43 percent) FinCEN received between February 14, 2014, and August 8, 2014, were termination SARs, indicating the bank deemed it necessary to terminate its relationship with these entities in order to maintain an effective anti-money laundering compliance program. In other words, almost the same number of institutions severed ties to marijuana businesses within the period analyzed as those that provided services. In April 2015, Dynamic Securities Analytics, which provides quantitative transaction analysis, reported that the percentage of non-suspicious marijuana-related SARs—filed solely because of the illegality of marijuana production, distribution and sales at the federal level—increased by 146 percent between August 9, 2014, and January 26, 2015, while reports of termination decreased to 36 percent. The more than doubling of these non-suspicious SARs indicates financial institutions want to capitalize on this burgeoning industry, but still need more information about their potential business partners.

Although federal guidelines and state laws provide some protection to those considering entering the market, they are only a starting point. Before issuing licenses and serving these operations, states, financial institutions and others must fully understand the backgrounds of the individuals applying for the licenses as well as their partners. They must also have a clear understanding of the sources of funding both within and outside of the United States. It is critical to investigate all dispensaries and growers before licensing to avoid any financial misconduct and to identify any criminal history or ties to organized crime, fraud or other corruption. Watchdog groups, citizens, media, law enforcement and other stakeholders will be carefully observing to ensure those involved in this business are beyond reproach.

The risks of fraud in the medical marijuana industry are clear and pervasive. States, banks, private equity firms, insurance companies and others could unknowingly enter into a financial relationship that could prove disastrous without thorough domestic and international due diligence investigations being completed on the dispensaries, growers and their sources of funds. Growers and dispensary owners could have significant financial or legal problems, ties to U.S. or international organized crime, or a host of other issues. Those doing business with such entities could face criminal prosecution, financial ruin and public embarrassment, leaving nothing but pipe dreams behind.

Jeffrey Cramer is a Senior Managing Director and head of Kroll's Chicago office. Jeff joined Kroll following a distinguished career as an Assistant United States Attorney in the Northern District of Illinois, Eastern Division. He has investigated a broad range of cases, including corporate fraud, organized crime, money laundering, RICO, foreign terrorist organizations, public corruption, securities fraud, and regulatory and export violations.

Finding treasures hidden in bankruptcy fraud

Bankruptcy investigators undeterred by uncooperative debtors, missing records and time constraints

By John Slavek, Managing Director and Jordan Lazarus, Senior Associate

Over the past year, bankruptcy fraud has been repeatedly splashed across headlines following the successful prosecution of several multimillion-dollar cases. As a consequence, bankruptcy fraud investigations may begin to sound routine and straightforward. In reality, recognizing and proving bankruptcy fraud is a difficult and time-consuming process. Even a detailed inquiry may result in a dead end and ultimately yield more questions than answers.

The majority of bankruptcy fraud allegations involve the concealment of assets from the bankruptcy court and appointed representatives. Activities that will likely lead to a charge of bankruptcy fraud include:

- Diversion of funds from the debtor to a non-debtor prior to the filings
- Failure to report all means of income by the debtor on bankruptcy filings
- Undervaluing non-exempt assets in a manner which prohibits them from being liquidated

Searching for these activities can be difficult in any fraudulent context. Scrutinizing debtors who are concealing the true value of their assets becomes even more problematic in the bankruptcy setting. For example, of the 44 bankruptcy fraud investigations initiated in 2014 by the Internal Revenue Service[1], only 12 indictments were filed, of which only eight cases resulted in sentencing.

Consider the most common challenges that confront financial investigators in cases of alleged bankruptcy fraud:[2]

- **Uncooperative and disgruntled debtors**
  Filing for bankruptcy is often the culmination of a series of damaging events for the debtor. If a trustee feels that an examination of a debtor's financial activity is necessary, it often falls on the investigator to work directly with the debtor. Debtors are typically in a state of distress and prefer to move through the bankruptcy process as quickly as possible while attempting to stabilize their financial status. The last thing they want to deal with is a forensic investigation into their financial affairs. This can lead to an adversarial relationship, and as a result debtors can be antagonistic, refuse to respond to requests for documentation, and sometimes exhibit threatening behavior in order to avoid the investigation. In many cases, the more stubborn the debtor is, the higher the likelihood of unveiling deceptive activity.
- **Seeming lack of available funds for a comprehensive forensic investigation**
  When debtors file under Chapter 7 bankruptcy, they often have limited non-exempt assets. These assets are used by the bankruptcy trustee to pay professional fees and distribute the remaining funds to creditors. At the beginning of a matter, the trustee usually performs a cost/benefit analysis to determine if bringing in accounting experts is worth the cost. In many cases, the answer should be a resounding "Yes!" Experienced professionals can look at a set of transactions and diagnose whether or not an investigation is warranted. If the investigator finds that "low hanging fruit" exists, these assets are often the first to be collected by the trustee, thus limiting the financial cost to the estate while maximizing the return. For matters that require a deeper understanding, investigators will carefully consider what aspects of a case need to be analyzed and focus their efforts there. This process limits the fees incurred while bringing about the best possible return on the trustee's investment in an expert.
- **Missing and/or incomplete records**
  Commonly, debtors lack the customary financial records needed for an investigation. Although the bankruptcy trustee has the power to file subpoenas to recover records, this process can take weeks or months. In addition, the absence of supporting documentation severely hinders the ability to actually prove that the concealment of assets has occurred. In an ideal forensic inquiry, the investigator has access

to complete and reliable business records with little interference by the client. Unfortunately, this scenario is more the exception than the rule in a bankruptcy investigation. Thus, the gathering of information from independent outside sources (banks, customers, vendors, etc.) is an integral step in the fact-finding process.

- **Limited timeframe**
  The timeline in a bankruptcy investigation can often be a double-edged sword. On the one hand, the trustee commonly has two years from the petition date to file adversarial proceedings in an attempt to recover assets. This period would appear to give the financial investigator a sufficient amount of time to review records, take depositions and fully investigate a set of suspicious transactions. On the other hand, the more time goes by, the less likely it is that a discovered asset will be available for recovery. For example, assume a debtor transferred a significant amount of money to a family member before the bankruptcy filing. The trustee takes 18 months to explore this transfer due to insufficient business documentation and a disinclined debtor and finally decides to file suit to reclaim this money. However, in the meantime, it is likely that the family member disposed of the funds and is unable to recompense the trustee. In this situation, a delay in the timeline led to a missed opportunity for an avoidance action against a related party.

Bankruptcy fraud requires specialized forensic investigative skills

Forensic accountants investigating potential bankruptcy fraud need to possess three critical skills:

1. **Case and time management.**
   In a typical financial investigation, the client suspects that a loss or theft has occurred and instructs the investigator to scrutinize specified areas. The opposite often occurs in a bankruptcy as the trustee generally does not know what potential assets may have been concealed and is relying on the financial investigator to uncover hidden assets. The related litigation may span several years and demand a high level of case-status management. Additionally, knowing when to stop investigating a suspect area is essential for effective time management.

2. **Basic familiarity with the debtor's business.**
   For many assignments, possessing a fundamental understanding of a target's specific line of work is not a prerequisite for a successful investigation. In bankruptcy probes, the opposite can be true. The investigator should be fairly knowledgeable regarding the debtor's type of business and typical vendors that are used in that industry. In addition, familiarity with key financial ratios commonly used in the trade is significant when analyzing tax returns and business records.

3. **Analytical thinking and investigative mindset.**
   An accountant who is exploring the potential concealment of assets must often uncover obscure information and piece together a complex puzzle. Records may be unavailable or incomplete, and debtors tend to be unaccommodating. The forensic investigator must be able to read between the lines and demonstrate when deceptive financial transgressions have indeed occurred.

The world of bankruptcy fraud is fraught with uncooperative debtors, incomplete records, a seeming scarcity of assets to fund comprehensive forensic investigations and compressed timeframes. Although these investigations are challenging, the recovery of hidden assets benefits all parties harmed by the concealment. By engaging financial investigators with proven experience in bankruptcy matters as soon as possible after the filing, trustees can best protect everyone's interests.

REFERENCES

[1] http://www.irs.gov/uac/Statistical-Data-Bankruptcy-Fraud

[2] These situations pertain primarily to cases filed under Chapter 7. This type of bankruptcy is the most severe in that it normally requires a complete liquidation of the debtor's non-exempt assets. A trustee is appointed to manage the case process and oversee the insolvency. After liquidation, the resulting value is used to pay the creditors and any professional fees.

John Slavek is a Managing Director in Kroll's Philadelphia office. Since joining Kroll in 1998, John has helped clients confront a wide range of finance and accounting issues, including corporate fraud, embezzlement, business income losses, bankruptcy, contractual disputes and internal control evaluation. He also has extensive experience working on due diligence projects, investigating financial statement manipulation and quantifying potential lost profits.

Jordan Lazarus is a Senior Associate in Kroll's Philadelphia office. His experience includes investigations of financial misconduct as well as the reconstruction of accounting transactions. During his time with Kroll, Jordan has focused his attention heavily on detailed forensic accounting matters, investigations dealing with possible FCPA violations and the drafting of expert reports dealing with these matters.

Technology's impact on integrity and business practices

By Peter J. Turecek, Senior Managing Director and Katy F. Shanahan, Associate Managing Director

Gone are the Mad Men days of two-hour extended business lunches and clients or colleagues being perfectly content to wait for a reply to their requests or questions. Today, business lunches, when jam-packed schedules even permit, often include iPhones and BlackBerries positioned as if part of the place setting. And if you actually end up taking a few hours—or days—to respond to a call, email or instant message, you risk being considered unprofessional, unresponsive or impolite.

Smartphones, tablets, laptops, the cloud and the like have quite literally untethered employees from their desks. However, one of the most problematic tradeoffs for this "freedom" has been employees steadily bombarded with informational data points from all sides and at all times—and always under pressure to respond at a moment's notice. This frenetic pace and fast-flowing streams of information in a highly mobile environment have created dangerous pitfalls for companies. One of the greatest of these is when members of the C-suite are less involved with the details of the business and instead rely on lower level professionals to raise critical points to their attention.

For example, a recent news article profiled the CEO of a major publicly traded company who said he won't open bulky spreadsheets anymore, desiring instead a synopsis of key points. This isn't necessarily a bad thing—the CEO is on the move visiting numerous work sites and clients, working to improve the business. For this arrangement to be successful, however, requires confidence in not only the capabilities, but also the integrity of those producing the data and creating the summaries.

But of course, there's the rub. In this new way of doing business, largely accepted across the globe as the norm, how can companies acquire that measure of confidence needed to make this system work?

First and foremost, companies must have a strong culture of ethical behavior demonstrated at all levels, both internally and externally. Management's tone at the top is critical to the success of implementing this culture. In word and deed, they should send a consistent message that ethical behavior is a job requirement, and unethical behavior is a career-limiting choice.

Internally, staff and professionals must be vetted not only to confirm their experience and expertise, but also for integrity issues. Companies also need to develop and adhere to a robust system of internal controls, including checks and balances, so that key details and critical information gain the attention they deserve and cannot be hidden by a rogue employee seeking to embezzle funds or steal product.

Additionally, training programs and initiatives around cyber and information security, compliance procedures and ethics must be conducted and tested on a regular basis. Losing smartphones, not properly protecting laptops while working remotely or in public places, and not password-protecting documents and other materials have all become much more common—and dangerous—since the advent of highly mobile work environments. As a result, companies have been investing heavily in security procedures, such as dual password requirements, locking of electronic devices after a shortened period of inactivity and requiring virtual private networks (VPN) use for employees' remote Internet access.

On the external front, proper compliance procedures should include vetting suppliers, vendors and other third parties for potential red flags, such as significant litigation, regulatory actions and other adverse findings relative to how the vendor or supplier conducts business. When onboarding these vital relationships, a company should also require acknowledgement of an agreement to the company's code of conduct. Investing in conducting these compliance-related activities upfront has time and again avoided detrimental issues later on.

Yet, despite proactive training programs and highly developed internal and external controls, problems can still arise. When they do, a company needs strong resources to obtain actionable intelligence about employees or business partners in order to make smart decisions. Some recent cases illustrate the dangers of getting it wrong and how these problems could have been avoided:

- A financial services company recently lost millions of dollars when a sophisticated cyber-phishing scam targeted a mid-level financial officer while senior executives of the company were at off-site meetings or on holiday break. The fraudsters were able to convince the financial officer to make multiple wire transfers out of the company to accounts in China before senior executives questioned the daily register of cash transfers. If the proper internal controls had been in place—double signatures on wire transfers, additional coverage over holiday breaks, training on potentially questionable email correspondence—the mid-level financial officer may not have moved forward with the transaction and the company might not have lost millions of dollars.
- In another case, the company hired a senior employee after an executive screening check was conducted. The senior employee then hired a consultant she knew, purportedly an expert in the field, to assist with a backlog of work. However, within months, the client learned of inappropriate activity and fired both the senior executive and the consultant. Kroll's investigation found that the senior executive's entire work history and most of her educational history was fake, including non-existent companies she had allegedly founded and a phony doctorate degree. In addition to properly vetting both employees before onboarding, the company should have also had consistent periodic ethics training and suitable internal processes for junior employees to report ongoing concerns about these individuals. Both may have helped the company avoid costly, post-situational litigation or prevented the problem at the outset.

As the times change, we have seen many cases where misplaced confidence in people or business systems can cause long-term damage. By reaffirming a commitment to ethical behavior and implementing comprehensive policies and procedures that continually reinforce that commitment throughout the entire organization, companies can go a long way to avoiding potential harm, internally and externally.

Peter J. Turecek is a Senior Managing Director and head of Kroll's Boston office. Based in New York, Pete is an authority in due diligence, multinational investigations and hedge fund related business intelligence services. He also conducts a variety of other investigations for clients in diverse industries related to asset searches, corporate contests, employee integrity, securities fraud, business intelligence and crisis management.

Katy F. Shanahan is an Associate Managing Director based in Kroll's New York office. She helps clients make risk management decisions about people, assets, operations and security through a wide range of investigations and due diligence services. Katy also manages a variety of complex multijurisdictional investigations, including large-scale due diligence assignments in support of IPOs and other transactional dealings, litigation support and corporate contests.

Will cryptocurrencies become tools for fraud?

By Alan Brill, Senior Managing Director

Introduction

Virtual currencies—which are not legal tender in any country and are not issued or backed by any government—have become an important factor in global funds transfers. But features associated with these so-called "cryptocurrencies," such as transaction anonymity and irreversibility of payments, have made them extremely attractive to cyber-criminals, drug dealers, money launderers and those involved in global fraud.

This article is based on a paper previously published in the Spring & Fall 2014 issue of Defense Against Terrorism Review (DATR), published by the NATO Centre of Excellence – Defense Against Terrorism (COE-DAT).

What is cryptocurrency and how does it work?

Cryptocurrency goes by many generic names. It is often referred to as virtual currency or as non-fiat currency. Perhaps the simplest definition comes from FinCEN: "'virtual' currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."

Bitcoins are a common example of a cryptocurrency. Bitcoins are not issued by a central bank or government, but rather may be purchased from a Bitcoin exchanger. Bitcoin exchangers accept conventional currencies and exchange them for Bitcoins based on a fluctuating exchange rate. Once acquired, the Bitcoins are stored in a digital wallet associated with "the user's Bitcoin 'address,' analogous to a bank account number, which is designated by a complex string of letters and numbers."

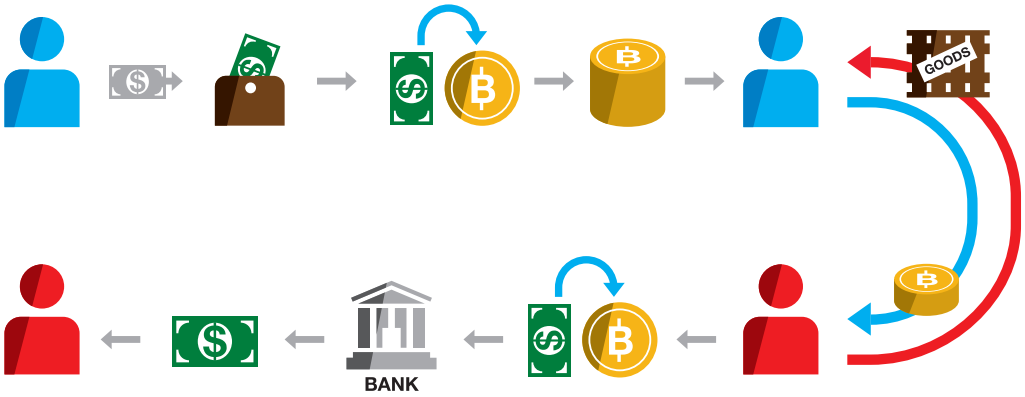
A Bitcoin transaction, which takes the form of a transfer of value between Bitcoin wallets, is recorded in a public ledger called a "blockchain." "To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network."

The chart below provides a simple overview of a transaction using a virtual currency (a Bitcoin for purposes of this example).

Person A wants to pay Person B for some product or service. Person A may be able to go directly to a money exchanger (who will exchange a sovereign currency for Bitcoins) or may have to go through a money transmitter to get it to the exchanger. The Bitcoins go into Person A's virtual currency wallet. Person A transfers them to Person B. Person B then can go through a money exchanger to get currency which can be deposited in a bank.

Why is cryptocurrency attractive to the fraud, money laundering and criminal underground?

If you were a fraudster, a money launderer or a criminal who wished to use the Internet to move funds globally to support your drug dealing or human trafficking operations, what characteristics would you want in a value-transfer tool?



- **Anonymity** – You would certainly want a system that did not require you to prove your identity and to have that validated identity tied to all of your transactions.
- **Global Reach** – The system should permit money to be transferred from anywhere to anywhere, and in any amount. You also want the ability to carry out transactions through third countries with which you have little or no connection.
- **Speed** – The system should carry out the transfers quickly, preferably within seconds. The faster the transaction, the less chance that it can be intercepted and blocked.
- **Non-Repudiation** – Transactions should be immediately final. The person sending the money should not be able to "un-send" it or reverse the transfer.
- **Difficult for Authorities to Track Transactions** – Obviously, you want a system that is not going to be an open book for the authorities to use to track your transactions or the actions of your group.

Cryptocurrency and unlawful transactions: the current state of affairs

The very characteristics of cryptocurrencies that make them attractive to fraudsters, terrorists, money launderers and criminals pose challenges for law enforcement and regulators. Two recent cases are Liberty Reserve and Silk Road.

The case of Liberty Reserve

In what is described as possibly the largest online money laundering case ever brought by the U.S. government, in May 2013, federal prosecutors charged Liberty Reserve, a currency transfer and payment processing company based in Costa Rica, with allegedly laundering billions of dollars, having conducted 55 million transactions that involved millions of customers around the world.

Liberty Reserve users were required to make any deposits or withdrawals through the use of third-party exchangers, "thus enabling Liberty Reserve to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail." Another key feature of Liberty Reserve transactions was that they could not be repudiated.

The case of Bitcoin and Silk Road

For approximately two and a half years, an underground website known as Silk Road "was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over a hundred thousand buyers, and to launder hundreds of millions of dollars derived from these unlawful transactions." One of the two major ways that Silk Road sought to operate beyond the reach of law enforcement was by requiring "that all transactions on Silk Road be paid with Bitcoins, an electronic currency that is as anonymous as cash."

Silk Road operated from January 2011, when it was established, until October 2, 2013, when the website was seized by law enforcement. In all, Silk Road is alleged to have generated the Bitcoin equivalent of "approximately $1.2 billion in sales and approximately $80 million in commissions." The alleged mastermind operator of Silk Road was ultimately convicted of multiple federal crimes.

Conclusion

Virtual currencies represent a challenge for law enforcement and every national government. Their promise to provide fast, safe and low-cost global funds transfers must be viewed relative to the risks associated with these currencies being used to facilitate and obfuscate transactions related to criminal activities, including money laundering, trading in illicit drugs and global fraud.

You can find the white paper in its entirety, including reference notes, at kroll.com.

Alan Brill is a Senior Managing Director and founder of Kroll's high-tech investigations practice. Alan consults with law firms and corporations and has led engagements that range from large-scale reviews of information security and cyber incidents for multibillion-dollar corporations to criminal investigations of computer intrusions, Internet fraud, identity theft, misappropriation of intellectual property, cases of internal fraud, data theft and sabotage.

Protect your systems: Five cyber attack realities to guide you

By Jonathan Fairtlough, Managing Director

You know you're a target. You've been told by many different white papers, handouts and flyers that cyber security must be used to protect your company from attacks. So, you decide to be proactive in your security approach and make risk-based decisions. And yet, a Google search on the subject will uncover hundreds of checklists, guidelines and products—all of which claim to solve a different security concern or problem. The risks seem endless, and the solutions impossible to wade through. Where do you start?

Start with these five cyber attack realities. Properly understood, they provide a guide to your next step in managing this risk.

1 **There is no turnkey cyber security solution**
There is no one solution that will protect all of your systems without your spending more time, effort or money. Cyber security is a difficult, time-consuming and ongoing process. The key to success is to balance the impact and cost of security with the actual risk posed. Kroll calls this balancing process "incident risk management." Start off with an assessment of the risks in your existing systems and focus your security accordingly.

2 **Build a fortress, but secure it from the inside**
We often see companies build protection around their systems that are similar to the fortresses built in medieval times. These fortresses often fail because the cyber attacker, when faced with defenses, does not try to break through them; instead, the attacker examines your security to uncover ways to walk right in.

Now, this does not mean you abandon the walls. Rather, the lesson that Kroll has discovered over the years is that you need to use all tools, with the most important, must-have safeguards being:

- Strong external security
- In-place internal monitoring systems

Here at Kroll, we have worked with numerous companies that invested in products to block continuous attacks. What we have noted, however, is an overall lack of investment in internal monitoring of systems, or what we call "end point threat monitoring."

End point threat monitoring is the use of software to record user activities within a network and flag any suspicious activity that may be indicative of a type of attack.

Failure to have end point threat monitoring in place will expose you to:

- An attack that lasts longer and is harder to catch
- A deep attack that will cost you more lost data
- No early warning signs that could have prevented the attack
- Costly repercussions from the type of attack
- Significant legal and regulatory liability

3 **Data loss is a symptom of a bigger problem you must investigate**
The fact that your company has lost data and must notify customers is the symptom of a larger problem, not the disease itself. You need to find the source of the problem. It could be an external hack, employee malfeasance or poor internal controls allowing for negligence. Data loss requires an investigation, not just notification. You need an investigation not only to find the source, but also to explain to the regulator how you have fixed the problem.

4 The attacker often stays in your system after the attack

Always assume that the attacker is still in your system. The goal of online attackers is to stay within a system for as long as they can. If they are driven out, then they are going to try to come right back in, often with user accounts they have set up on the system. Attacked networks need to be monitored until all users and processes are validated. End point threat monitoring is a key part of that solution.

5 Cyber fatigue is real, but not an excuse for inaction

It's easy to become fatigued at the thought of cyber security. With so many things to do and to learn, you can lose sight of the benefits. If the process does become too overwhelming, remember this: Each step your company takes to protect itself makes it that much more difficult for attackers. They will move on to an easier target—one without as much security in place. Don't worry about perfection. Rather, make sure you are hitting the standards, protecting key systems and planning to learn and grow. The more attempts you make at cyber security, the better your chances are to stay protected.

Jonathan Fairtlough is a Managing Director in Kroll's Cyber Security Practice. Jonathan leads teams that provide comprehensive investigative services for digital forensics, data breach response and complex cybercrimes. He joined Kroll after a distinguished career with the Los Angeles County District Attorney's Office, where he was involved in many high-profile cases as a prosecutor as well as co-founder of the office's High Technology Division.

Real estate dealmakers and industry must prepare for due diligence crackdown

By Michael Cabonargi, Associate Managing Director and Mark Skertic, Associate Managing Director

Federal law enforcement is evaluating a proposed rule to combat money laundering through shell companies. If adopted, the rule would dramatically expand and deepen the compliance and due diligence required from financial institutions to identify beneficial owners—as well as the legal owners—of accounts. Legal and real estate experts predict that high-profile investigations and enforcement actions may be imminent—and the real estate industry must prepare now.

The big picture: New due diligence requirements

Currently, financial institutions exercise their own judgment in making risk-based assessments of whether to require beneficial owner information for legal entity accounts. Banks, broker-dealers, mutual funds, futures commission merchants and introducing brokers in commodities are already required to have robust policies and procedures to conduct customer due diligence and comply with recordkeeping and reporting requirements, such as the filing of suspicious activity reports.

In July 2014, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued a notice of proposed rulemaking that would expand and reset this compliance burden. The proposed rule would require banks, real estate professionals and others to identify and verify the identity of beneficial owners of entity customers.

The new rules could significantly affect real estate investment, where shell companies are sometimes used to obfuscate the ultimate owners of property. FinCEN Director Jennifer Shasky Calvery recently used her comments at an anti-money laundering forum in May 2015 to update attorneys and compliance professionals on the status of the proposed rule, especially as it relates to potential money laundering through real estate transactions.

"As far back as 10 years ago when I was working as a prosecutor, so many of my very own investigations were stalled by an inability to follow the money," Director Calvery said. "And inevitably shell companies were involved. So when people ask 'why beneficial ownership' and 'why now?' what I really want to say is 'why not 10 years ago?'"

Who is a "beneficial owner" for purposes of identification?

The proposed rule requires the identification of all individuals that meet either the "ownership test" or "control test"—either owning 25% or more of the equity interests of the legal entity customer or having significant responsibility to control, manage or direct the legal entity customer (such as an executive officer).

This requirement to identify natural persons will force banks and others to peel back multiple corporate layers during the identification process. Acknowledging the difficulties involved, FinCEN is nevertheless unambiguous on the requirement to identify actual individuals "regardless of how many corporate parents or holding companies removed the natural person is from the legal entity customer."

Impact on the real estate industry

FinCEN Director Calvery brought the proposed FinCEN rule into the field of real estate transactions when she further stated "we need to ensure transparency in the area of real estate." She referenced the February 2015 investigation by The New York Times, "Towers of Secrecy." It concerned the use of shell companies to purchase high-value condominiums and real estate in New York City. The series found that shell companies own significant percentages of units in high-profile New York buildings, including Trump International (57%), One57 (77%) and Time Warner Center (64%).

In the Time Warner Center alone, after piercing through the shell companies and identifying the actual beneficial owners, The Times found 37% of the units are owned by foreign nationals, including government officials and close

associates of officials from Russia, China, Kazakhstan, Malaysia, Colombia and Mexico. At least 16 of the beneficial owners have been the subject of government inquiries into financial fraud, housing and/or environmental violations. Four owners had been arrested and another four owners had been penalized or fined for illegal activities.

The Times' findings are consistent with what federal investigators have found. "FinCEN continues to see the use of shell companies by international corrupt politicians, drug traffickers, and other criminals to purchase luxury residential real estate in cash," said Director Calvery. "Our information shows funds transfers in the form of wire transfers originating from banks in offshore havens at which accounts have been established in the name of the shell companies."

What do real estate professionals need to do now?

So, federal law enforcement and regulators are aware of the problem and poised to take action. What do banks, real estate professionals, developers and their attorneys need to do now to be ready for the inevitable?

1. **Know where to start and what is required at minimum.** The proposed FinCEN rule notes that covered financial institutions need not conduct the analysis themselves to identify the beneficial owners, but generally may rely on the representations of the legal entity customer. However once disclosed, the proposed rule requires that covered financial institutions actually verify the identity of all disclosed beneficial owners in the same manner as current customer identification requirements (e.g., by collecting a driver's license).
2. **Put in place services and processes in the event the identity of the beneficial owners cannot be verified.** The proposed rule explicitly states "[a] financial institution must also include procedures for responding to circumstances in which it cannot form a reasonable belief that it knows the true identity of the beneficial owner." Institutions will want to retain standby due diligence and investigatory services, to be used as needed.
3. **Organize and prepare these processes sooner rather than later.** Industry leaders agree that the real estate transaction deal flow can slow or freeze up entirely if counsel and developers do not have the requisite revised due diligence procedures and safeguards in place and ready.

While the proposed rule and FinCEN's emboldened push for enforcement will motivate real estate dealmakers and banks to strengthen their in-house compliance departments, the industry is already struggling with a shortage of experts capable of untangling complicated shell-company deals in order to identify the actual beneficial owner.

Thus, this stronger and more assertive push by federal law enforcement to fight money laundering and corruption in real estate transactions will also likely force dealmakers to factor in extra time to ensure compliance and take steps to ensure they have the expertise in place to provide the increased level of scrutiny FinCEN is prepared to require.

* This article is condensed from a white paper that can be found on kroll.com.

Michael Cabonargi is an Associate Managing Director in Kroll's Chicago office. As a former attorney in private practice with corporate law firms as well as a senior attorney and prosecutor with the U.S. Securities and Exchange Commission (SEC), Michael has uncommon insight into the dynamics of complex financial investigations, including those involving regulatory inquiries/litigation, fraud, insider trading and Ponzi schemes.

Mark Skertic is an Associate Managing Director in Kroll's Chicago office, where he manages a variety of complex investigations. His expertise spans due diligence matters, proxy fights and hostile takeovers, litigation support, competitive intelligence, internal investigations, intellectual property disputes, computer forensic investigations and other security matters. Prior to joining Kroll, Mark was an award-winning investigative reporter and editor.

Fraud is a “risky” business

By Joseph A. Spinelli, Senior Managing Director

It seems every day we read about organizations subjected to frauds resulting in massive investment losses, incarceration of employees and reputational damage. The U.S. Sarbanes-Oxley Act of 2002 and the U.S. Federal Sentencing Guidelines of 2005 increased management’s responsibility to design and implement a fraud risk management program and “no tolerance for fraud” attitude.

All effective fraud risk management programs begin with the boards of directors of an organization ensuring overall high ethical behavior, regardless of its status as private, public or not-for-profit; its size; or the industry it conducts its business. The board of directors’ role is of great importance because most major frauds are committed by senior representatives of an organization in collusion with other employees. Thus the board of directors must ensure that its own governance practices set the tone for fraud risk management, and that management effectuates policies that encourage ethical behavior, including providing a mechanism for employees, agents, vendors and customers to report violations of those standards without fear of retribution.

It has been my experience that most organizations have some form of written standards and procedures to manage fraud risks. However, very few have a fraud risk management program that provides the organization with the tools to manage risk consistent with regulatory requirements, and to design a wide-ranging program that encompasses controls to enjoin, detect and respond to incidents of fraud or misconduct. An effective fraud risk identification process should include an assessment of the incentives, opportunities and rationales to commit fraud. Oftentimes employee incentive programs are road maps as to where fraud is most likely to occur.

An effective fraud risk identification process should include an assessment of the incentives, opportunities and rationales to commit fraud.

In summary each organization that designs and implements a fraud risk management program should be certain to define the following elements:

- Roles and responsibilities
- Fraud awareness training
- Fraud risk assessment
- Reporting procedures and whistleblower protection
- Investigation procedures
- Disciplinary action for violators of procedures
- Corrective actions
- Continuous auditing and monitoring

The benefit of an implemented fraud risk management program will always exceed its cost. The board of directors should ensure the organization has adequate controls in place and recognizes their oversight duties and obligations in terms of the organization's sustainability and their roles as fiduciaries to shareholders. The board in conjunction with management is directly responsible for developing, executing and mitigating controls to address fraud risks while ensuring controls are effectuated by adept and objective individuals. Regulators have "zero tolerance" for anything less!

Joseph A. Spinelli is a Senior Managing Director with Kroll's Investigations and Disputes practice, based in New York. In a career spanning more than 30 years across both the private and public sectors, Joe has been a pre-eminent leader in multiple fields, including white collar investigations, anti-bribery and corruption, FCPA, risk management, monitorships, criminal investigations and forensic accounting.

Canada overview

Canadian participants reported some improvement in fraud figures since the previous survey as well as a comparatively low overall prevalence of fraud (65% against a global average of 75%). However, the picture is not so rosy in all areas. Over the last year, Canada had the highest average loss to fraud (1.0% of revenues) of any of the countries covered in this Global Fraud Report. It also had the highest incidence for theft of physical assets (26%), as well as the second highest figures for both vendor or procurement fraud (23%) and management conflict of interest (19%).

Canadian respondents report very high rates of insider involvement compared to the other countries reported on. Where a company was a victim of fraud with a known perpetrator in the past year, in 60% of cases Canadian respondents said that a senior executive or middle manager had played a leading role and the same number reported that a junior employee had also been involved. In both cases, this was the highest for any country.

Meanwhile, however, Canadian companies are not convinced they have a problem. Only 19%, for example, believe that they are highly or moderately vulnerable to management conflict of interest, compared to 36% for the survey as a whole. Similarly, just 48% believe themselves vulnerable to theft of physical assets, compared to 62% overall. As noted above, in both cases Canada had one of the highest levels of these crimes.

This attitude may be responsible for a comparatively low level of resources being directed toward combating fraud by Canadian companies. One in six said that lack of budget for compliance had increased their fraud exposure in the past year, the highest figure for any country reported on. Investment plans for the future show the same problem. Canadians are less likely than average to report planned investment in all but one of the anti-fraud defenses covered by the survey over the next year. The only exception, IT security, was marginally above the average (68% compared to 67%). Probably most worrying of all given the high incidence of management conflict of interest and fraud perpetrated by senior executives, only 19% plan to invest further in management controls, compared to 39% for the survey as a whole.

CANADA REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	65%	69%
LOSS Average percentage of revenue lost to fraud	1.0%	1.7%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Theft of physical assets or stock **(26%)** ■ Vendor, supplier or procurement fraud **(23%)** ■ Management conflict of interest **(19%)**	■ Information theft, loss or attack **(29%)** ■ Management conflict of interest **(29%)** ■ Theft of physical assets or stock **(20%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**77%**	**83%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(40%)** ■ Increased outsourcing and offshoring **(23%)** ■ Lack of budget/resources for compliance **(17%)**	■ IT complexity **(31%)** ■ Increased collaboration between firms **(31%)** ■ Increased outsourcing and offshoring **(31%)**

Down to the wire

By Peter McFarlane, Managing Director, Deborah Gold, Managing Director and Jennie Chan, Managing Director

In the past year, Kroll Canada has seen a significant increase in wire transfer fraud, costing its victims time, money and significant operational disruptions. One of the greatest worries for companies, however, is the possibility that they were being targeted from the inside.

In each case where Kroll was retained, the perpetrators seemed to have an uncanny knowledge of the victimized company, including its corporate structure, such as names and positions of executives as well as employees within the treasury and accounting functions. This in-depth knowledge triggers concerns regarding internal involvement or collusion. However, companies should also realize that the use of social media, professional networking sites such as LinkedIn and a company's own website can make it easy to ascertain information about the company's executives and how the company operates.

The fraud usually starts with a single email—often ostensibly from a senior executive—requesting a fund transfer. In most cases, the email contains a chain with what appears to be legitimate prior communications between senior executives, thereby strengthening the credibility of the message. Bolstered by this apparently legitimate string of executive communications, it is not unusual for the recipient to confirm and facilitate the fraudulent transfer request.

One mechanism used to carry out the fraud is to slightly modify the domain name in a manner that will usually go undetected by the recipient. For example, the perpetrator would use "@krolll.com" instead of "@kroll.com". It's easy to see in a case like that how a recipient could miss the different spelling, especially if the sender is a senior executive.

Growing and widespread problem

In 2014, wire transfer fraud was the number one mass-marketing fraud (MMF), as calculated by dollar loss, reported to the Canadian Anti-Fraud Centre (CAFC), to the tune of more than $22 million. "Only one to five percent of MMF victims report to the CAFC," says Daniel Williams of the Royal Canadian Mounted Police, who is senior call taker supervisor at the CAFC. "So, sadly, we are all too certain the actual numbers are much higher." The second most-reported fraud in 2014, for comparison, involved dollar losses of just under $13 million.

The problem is prevalent enough that, in early 2014, the Toronto Police Service issued a news release warning companies and individuals of "a number of incidents [requesting] large sums of money to be transferred by email."

In the U.S., the scam is known as a business email compromise (BEC). According to a January 2015 alert from the FBI, it had received BEC complaints from every state and 45 countries. The total dollar loss between October 2013 and December 2014, based on the cases of which it was aware, was approximately $179.75 million in the U.S., and a combined loss of almost $215 million worldwide. "The FBI assesses with high confidence the number of victims and the total dollar loss will continue to increase," the alert said.

A simple but sometimes compromised solution

The way to combat wire transfer fraud would seem quite clear, straightforward and obvious: put in place proper policies and procedures. Indeed, having these policies and procedures is critical, but wire fraud highlights a persistent security weakness—our human nature. Often, security controls are overridden simply due to our desire to please others, particularly those in positions of authority. In the cases we've seen, when employees receive requests from senior executives, the motivation to assist the person higher in rank outweighs the need to stop and validate that the request is legitimate.

The way to combat this possibility is for a company's most senior managers to make it absolutely clear to everyone involved in approving wire transfers that no one, no matter their rank, can override policies or proper procedures. When that message is communicated clearly, the chance of being defrauded in this manner is reduced significantly.

Red flags to identify potentially fraudulent wire transfer requests

- **Unusual or vague transaction details:** The transaction is described in vague terms (e.g., "strategic marketing advice") or referenced as a confidential matter known to senior management (e.g., "confidential joint venture investment"). Instructions regarding recording of the transaction are also vague (e.g., "corporate marketing").
- **Unknown beneficiary and round-sum amounts:** The beneficiary is typically a person/entity unknown to the organization and may reference a jurisdiction in which the organization typically does not conduct business. Round-sum amounts, such as "$200,000," should raise suspicions, although many fraudsters are aware of this and often avoid them.
- **Requirement to circumvent normal protocols:** A pretext is often presented to justify the need and urgency to circumvent normal protocols. These include reasons such as the funds must be received before end of business the next day to close a confidential transaction, avoid penalties or avoid seizure of product.
- **Absence of required supporting documents:** Normal wire transfer requests should be supported by appropriate documentation available to both those preparing and approving the transfer. Fraudulent requests often state supporting documents will be provided later or were provided to the CEO or other senior executives.
- **Non-standard email format:** Any irregularity in email headers, footers and content such as John.Doe@acme.com rather than the standard format jdoe@acme.com or use of an atypical font or email footer suggest that it could be a fraudulent communication (in addition to a false email domain).

Five strategies to avoid fraudulent wire transfers

An organization can employ strategies over and above basic internal controls to avoid processing fraudulent wire transfers.

1. **Enhanced training and awareness.** All relevant employees should receive training periodically to ensure they are fully aware of corporate policies, the prevalence of fraudulent wire transfers and the red flags indicating a potential fraudulent request. All communications from banks or agencies regarding wire fraud scams should be circulated.
2. **Establish escalation protocols.** Employees should be provided with predefined escalation protocols if they have concerns regarding the validity of a wire transfer request. These escalation requests and subsequent approvals (or denials of approval) should be documented, including details of procedures undertaken to address the initial concerns.
3. **Establish protocols for rush or confidential wire transfer requests.** Predefined protocols should be established to accommodate legitimate rush and/or confidential transfers.
4. **Use IT filters to block fraudulent emails.** Existing IT systems can be used to block or flag unwanted emails, such as those emanating from domain names similar to that of the organization.
5. **Monitor domain registrations.** Conduct periodic searches to identify registered domain names similar to that of the organization. Suspect names can also be blocked.

Peter McFarlane is a Managing Director at Kroll and leader of the financial investigations team in Toronto. With more than 25 years of forensic accounting and investigative experience, Peter manages a wide range of complex financial investigations, litigation consulting, asset recovery and financial due diligence assignments for corporate and government clients around the world. Peter has investigated a broad range of fraud cases, including management and employee fraud, money laundering and funds tracing.

Deborah Gold is a Managing Director with Kroll, based in the Toronto office. Deborah provides due diligence solutions to support clients' commercial transactions, investments and regulatory compliance, and to help them manage legal, regulatory, financial and reputational risk concerns. She is an expert who has assisted clients with diverse aspects of anti-money laundering programs and FCPA compliance reviews.

Jennie Chan is a Managing Director with Kroll, based in the Toronto office. Jennie has more than 20 years of experience in complex financial and internal investigations on behalf of public and private corporations, governments and regulatory and law enforcement agencies. The breadth of her investigative expertise spans a broad range of issues including employee fraud, procurement fraud, secret commissions and allegations of corruption in Canada, the United States, Europe and Asia.

Brazil overview

In general, respondents from Brazil reported fraud prevalence roughly similar to that in the rest of the world. The overall figure (77% suffered from at least one fraud in the last year) was slightly higher than the global average (75%) while the financial loss (0.7% of revenues) was a little under the whole survey figure (0.8%).

Within this broader picture, though, some notable problems exist. Brazil had the highest reported rate of internal financial fraud (23%) of any of the eight countries covered in this report. In this group, it was also tied with Mexico for the second highest number of companies suffering some economic damage in the last 12 months (73%).

What really sets Brazilian respondents apart this year, though, is a below average intention to improve its defenses against fraud, even where executives know there is a weakness. For every anti-fraud strategy in the report, those queried are less likely than average to plan to invest. More striking, the number of respondents reporting that their firms plan to put money into management controls (20%) is less than that saying they suffered internal financial fraud during the last year. Similarly, the proportion of Brazilian respondents expecting their firms to invest in greater due diligence (20%) is below that reporting increased risk from greater outsourcing (23%). Finally, Brazilian respondents are the least likely of those from any of the reported-on countries to indicate that they will pay more for staff background screening (23%), even though 27% say that high staff turnover is increasing risk exposure.

BRAZIL REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	77%	74%
LOSS Average percentage of revenue lost to fraud	0.7%	1.7%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Internal financial fraud **(23%)** ■ Theft of physical assets or stock **(17%)** ■ Vendor, supplier or procurement fraud **(17%)**	■ Theft of physical assets or stock **(37%)** ■ Management conflict of interest **(26%)** ■ Vendor, supplier or procurement fraud **(23%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**80%**	**86%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(27%)** ■ Increased outsourcing and offshoring **(23%)**	■ High staff turnover **(42%)**

Are you prepared for Brazil's new anti-corruption policies?

By Snežana Gebauer, Managing Director

Investors around the world have always shown great interest in Brazil, and continue to do so despite recent economic and political turbulence. Brazil has a broad portfolio of opportunities in industries such as agribusiness, oil and gas, energy and, predominantly, infrastructure. All of these industries are to a different extent influenced or controlled by the Brazilian government, and as a result are intertwined with Brazilian politics. This makes it more challenging for foreign investors to enter the markets and to navigate an unfamiliar political environment.

During this past year, Brazil has seen a colossal shift of the corporate and political landscape as a result of the highly publicized prosecution of corruption involving Brazil's oil giant, Petrobras, and the key players within the construction industry. The prosecutions have involved top executives at most of the companies in these promising industries as well as government officials in high-level positions. The prosecutions were the culmination of a mission to fight corruption that was started years ago and were preceded by the passing of Brazil's Anti-Corruption Law. Both events have been instrumental in changing the way Brazilian companies face and deal with corrupt conduct.

Despite the economic and political turbulence that Brazil is undergoing at the present—economic indicators are not as favorable as those of eight years ago and there is speculation whether or not the president will complete the end of her term—foreign investors remain interested in Brazil. Some even claim that this is a better time to invest than five or eight years ago, as the prices of Brazilian assets are attractive to investors from the U.S., Europe and Asia due to the devaluation of the real.

A key concern for foreign and local investors and their corporate management is preventing their business from becoming entangled in any corrupt activities and the attendant legal and financial liabilities and reputational damage. Kroll has seen a significant increase in awareness as well as efforts by companies to establish sound policies aimed at preventing and detecting corruption.

While multinational companies have been at the forefront in implementing compliance programs worldwide, and especially in Brazil after the passage of the Brazilian Anti-Corruption Law, Brazilian companies have been quickly trying to catch up by implementing compliance programs or improving their existing policies and procedures.

Based on our experience in Brazil, three key elements of an effective compliance program include:

- **Compliance leader with authority, independence and resources**
  Usually a chief compliance officer fills this role. Corporations that have successfully transformed their compliance culture have identified candidates with the appropriate experience, competencies, ethics and independence and placed them in positions of authority with a reporting line to stakeholders. Corporations that take a long-term view and see spending resources on compliance as an investment and not a cost tend to be more effective in providing appropriate support to their compliance leader.

- **Robust internal controls**
  Corporations that build compliance programs as part of an integrated effort with internal audit and risk management/control are more successful than those who have compliance departments operating in a more isolated manner. Corporations can build robust internal controls only if risk knowledge is shared throughout the organization and if the respective departments actively play a role in preventing and detecting corruption.
- **Increased awareness**
  A code of conduct is used by most organizations to establish and institutionalize their key compliance policies. An effective and frequent dissemination of an inclusive and practical code of conduct is the basis for creating awareness. To build and sustain a corporate culture that condemns corruption in the organization, corporations usually rely on a combination of frequent and interactive trainings that are incorporated in the key performance indicators of employees as well as corporate events dedicated to the compliance cause, including other events or campaigns.

Snežana Gebauer is a Managing Director and head of Kroll's São Paulo office. Snežana possesses deep understanding of the dynamics, practices, players and challenges in today's complex business world, particularly in emerging markets, and speaks five languages. She has managed sophisticated strategic intelligence gathering engagements in complicated cross-border transactions and challenging business situations in Latin America, Europe and the Middle East.

Mexico overview

Mexican respondents to this year's survey reported above average figures for both incidence and cost. The overall prevalence of fraud—80% of companies were affected at least once in the last 12 months—was higher than the global average (75%). Moreover, while the average economic loss was at the survey average of 0.8% of revenues, Mexico was tied with Brazil for the second highest number of companies suffering at least some financial damage (73%) among the eight countries covered in this report.

Looking more closely reveals particular problems. Mexican respondents reported the highest national rate of vendor or procurement fraud (23%) and the third highest one for misappropriation of company funds (10%). Companies are also having problems with their agents and intermediaries. Where a business had suffered a fraud in the past year and the perpetrator was known, 29% of Mexican respondents said that such an individual played a leading role, the second highest national figure.

Mexican respondents, however, may be underestimating their danger. For both vendor or procurement fraud and misappropriation of company funds, only 3% say that their firms are highly vulnerable, well below the figures for those who actually suffered such crimes in the last year.

Interest in defense is also relatively low: for eight of the 10 anti-fraud strategies covered in the survey, a lower than average number of Mexican respondents reported planned investment in the next year. One of the two exceptions was partner, client, and vendor due diligence—an obvious area of focus given high rates of vendor fraud—but here the difference between the number planning to invest and the overall average disappears with rounding (33% in both cases).

MEXICO REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	80%	63%
LOSS Average percentage of revenue lost to fraud	0.8%	1.9%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Vendor, supplier or procurement fraud **(23%)** ■ Theft of physical assets or stock **(23%)** ■ Information theft, loss or attack **(17%)**	■ Theft of physical assets or stock **(30%)** ■ Corruption and bribery **(25%)** ■ Internal financial fraud **(25%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**67%**	**93%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(23%)** ■ Increased outsourcing and offshoring **(20%)**	■ High staff turnover **(45%)**

The return of retail theft to organized crime

By Jim Faulkner, Managing Director

For decades, the established U.S. organized crime groups, such as La Cosa Nostra or the major "mob" families of New York and Chicago, conducted truck hijackings. These strong-armed attacks were conducted on drivers of trucks with containers holding expensive commercial goods, such as televisions and garments. The hijacked goods made their way onto the shelves of wholesalers and retailers throughout the United States and became one of the mob's principal sources of criminal revenue. Eventually, these hijackings and other "rackets" significantly diminished or became extinct due to the mob's expansion into the more lucrative drug world. Also, the families themselves largely retreated after major criminal prosecutions, such as those filed in the Southern District of New York.

Today, multiple phenomena are contributing to an equal if not greater amount of retail fraud or theft than in the days of the sensational mob hijackings. However, today's theft does not involve armed physical attacks on transporting conveyances, but rather organized rings engaged in transnational fraud, corruption and shipping schemes. Such rings are not run by the old Mafia dons, but by hardened criminals born out of other groups of immigrants.

The first phenomenon is the worldwide development of the open marketplace and, in particular, Latin American markets, which enjoy Free Trade Agreements and Trade Tariff Waivers with the United States. These agreements have helped countries such as Colombia and Mexico develop more productive manufacturing sectors and stronger economies, but have also had a dramatic effect on U.S. exports. The North-South shipment of stolen goods is enhanced by the volume of trade as well as the lack of tariffs to many Latin American countries, and the consequent dearth of inspections and export controls.

Moreover, there is a commercial incentive to ship those goods to Latin American markets: a PlayStation or LED television in many Latin American venues has far greater retail value than in the United States, due to a combination of high import fees and the relative unavailability of such goods in local markets. Indeed, foreign consumer goods in Latin American countries can cost up to three times more than the products cost in the United States. For example, according to Bloomberg Business, while the PlayStation 4 costs $400 in the U.S., the console costs the equivalent of approximately $1,700 in Brazil.

In February 2011, at the request of the National Retail Federation, the Department of Homeland Security (DHS)—which is responsible for the integrity of U.S. borders and the enforcement of export smuggling of contraband—established a pilot federal investigative task force based out of South Florida. That task force is responsible for the identification and prosecution of groups and individuals engaged in organized retail fraud and theft schemes, with particular focus on those aimed at shipping stolen goods to Latin America for sale.

Observations made by Kroll as a result of recent investigations, consistent with information shared by law enforcement, clearly indicate that this latest trend in transnational crime involves organized groups and appears to be growing in volume. The leaders of these groups tend to have extensive criminal backgrounds and are often related to other Latin American immigrant groups. They believe they are relatively safe in managing these international fraud/theft schemes, as law enforcement has yet to react fully to the trend. Violators know the potential criminal penalties are far less severe than for other types of crimes, for example, narcotics trafficking.

Given the large profits involved, the likelihood is that this criminal trend will only grow in volume and geography until governments make it a priority to investigate, map out and prosecute the leaders of this type of organized crime, while enacting legislation to enhance the criminal penalties. Until retailers pool resources to investigate and work together more effectively with law enforcement to eliminate this organized crime phenomenon, international retail theft will continue to grow and flourish in enjoyment of near complete impunity.

Jim Faulkner is a Managing Director and head of Kroll's Miami office. Jim joined Kroll after a distinguished career with the U.S. Department of Justice, where he ultimately served as the judicial attaché in Bogotá, Colombia, leading legal diplomacy efforts for U.S. prosecutors and federal agents and helping to coordinate a massive extradition and mutual legal assistance program. Jim has also prosecuted international drug trafficking rings, including two leaders of the largest terrorist organization in the Western Hemisphere.

Penetrating the offshore sector

By Glen Harloff, Managing Director

The following hypothetical case, a composite of cases appearing in the public record, is representative of the types of matters where Kroll is tasked to investigate financial fraud in the offshore sector. It illustrates the ways in which offshore havens have been used to divert significant capital from allegedly legal transactions across the globe.

A medium-sized European manufacturing company decides to expand its manufacturing facilities to Asia to improve its competitiveness. The CEO subsequently orchestrates the purchase of a facility for $9 million.

Move the clock ahead four years: the CEO has retired, there are serious issues with the Asian facility, and the company questions what exactly it bought. Enter Kroll, who is engaged by the company to investigate the matter and is able to determine that the actual purchase price for the Asian facility was $2.2 million and the balance of $6.8 million was diverted to a company domiciled in an offshore financial center (OFC). As is typical for an OFC, its public records indicate the date of incorporation, number, name of registered agent and status. So is this the end of the trail?

There are approximately 95 OFCs or tax havens located in the Caribbean, the United States (i.e., Delaware), Southeast Asia and the Pacific Ocean. Reports indicate that OFCs serve as domiciles for more than 2 million paper companies and thousands of banks, investment funds, insurance companies and most large registered vessels. OFCs range from developed jurisdictions, such as the Cayman Islands specializing in investment funds and Bermuda specializing in insurance, to the “aspirational havens” that have turned to finance to reduce their reliance on tourism and agriculture.

OFCs have been under tremendous pressure over the past decade or more to disclose information on assets they hold. To ease some of that pressure, the majority have agreed to the exchange of tax information on clients and their home countries. However, the pressure continues, with emphasis on curtailing tax avoidance/evasion, terrorist financing and proceeds of crime/money laundering. This does little to assist in the above scenario unless law enforcement can be convinced to investigate; however, this can be a tough sell when their priority is criminal prosecution versus trying to recover $6.8 million for a private company.

Obtaining information on the directors, officers and beneficial owner(s) of an offshore company means penetrating the records of the registered agent, who holds “the keys to the vault” and based on OFC secrecy laws, cannot disclose the information unless compelled by the courts. Fortunately, the courts have provided us with a tool, namely the Norwich Pharmacal or Discovery Order (Order). The Order places a duty on a third party to assist the aggrieved, even if the third party did nothing wrong. The rules are reasonable and straightforward and include:

- An allegation of wrongdoing/fraud
- A requirement for full disclosure of the facts both pro and con, as court proceedings are in camera
- Stipulation as to the documents that are required and why these documents are necessary/crucial in furtherance of the fraud, pending or actual litigation
- Reasonable to conclude that the documents are in possession of the third party
- Convincing the court that the information cannot be obtained from other sources or methods of investigation

While rules and procedures for obtaining an Order can differ between OFCs, it is a requirement to engage legal counsel in the OFC and wiser still to engage counsel with experience in obtaining Orders. Counsel should be familiar with the latest approach of the presiding court in these matters, and can present the matter to the court and seek to obtain the Order.

Let's go back to our case. After discussions and with the assistance of legal counsel, Kroll would be asked to prepare an affidavit telling the story of what it believed to have happened, the information required, the belief that the information was in possession of the registered agent, and all other avenues of investigation had been exhausted. In this hypothetical case, counsel presented the affidavit, the application for an Order and draft order to the court. The court agreed to issue the Order on the registered agent, which was subsequently served, and the information was provided within 10 days of the Order. To finish our story, the Order succeeded in producing crucial evidence that the CEO was the beneficial owner of the offshore company resulting in civil and criminal actions against the CEO.

The moral of the story: The offshore sector can be penetrated. The key is to conduct a thorough investigation and utilize all the tools and resources available, including engaging experienced legal and risk management partners.

Glen Harloff is a Managing Director for Kroll in Miami, Latin America and the Caribbean. Glen specializes in forensic accounting, investigations, litigation consulting and financial due diligence, with extensive experience in such areas as insolvency/bankruptcy, secret commissions and internal investigations. Glen has traced and secured assets relating to the proceeds of crime/money laundering throughout North America, the Caribbean, Europe, Asia and Africa.

Colombia overview

Colombia has a growing fraud problem, with the highest overall prevalence (84%) of any of the eight countries reported on in this survey. In this group, it also has the highest incidence of information theft, loss or attack (27%) and management conflict of interest (23%). It is also the only country reported on that saw an increase in the average loss to fraud (to 0.9% of revenues from 0.7%) so that, for the first time in one of our surveys, this figure is above the overall mean.

It is noteworthy, however, that as in the previous year, Colombia's fraud problem is focused on a few particular crimes, while others are being reported very little: for seven of the 11 frauds covered in the survey, the country's incidence was below average and the figure for theft of physical assets (17%) was the lowest of any country reported on.

The most pressing issue revealed in the survey is that Colombian companies need to take the threat from the top more seriously. Where a fraud had occurred in the previous year and the perpetrator was known, 44% of Colombian respondents said that senior executives or middle management had been involved—this is the second highest level among all countries surveyed this year. As noted above, management conflict of interest is also a more widespread problem in the country than in any other of those reported on.

On the other hand, the percentage of Colombian respondents saying that their firms were highly or moderately vulnerable to such a conflict of interest was only about average (37% compared to 36% overall). More striking, just 20% reported that their businesses would be investing in further management controls in the coming year, tied for the second lowest national figure and about half the average (39%). This even though only 13% report currently having such controls in place—the lowest for any country reported on. Without more attention to management, Colombia's fraud problems look unlikely to diminish.

COLOMBIA REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	83%	63%
LOSS Average percentage of revenue lost to fraud	0.9%	0.7%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Information theft, loss or attack **(27%)** ■ Management conflict of interest **(23%)** ■ Theft of physical assets or stock **(17%)**	■ Theft of physical assets or stock **(37%)** ■ Vendor, supplier or procurement fraud **(20%)** ■ Corruption and bribery **(17%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**63%**	**90%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(23%)**	■ Entry into new, riskier markets **(47%)** ■ High staff turnover **(47%)**

China overview

Seventy-three percent of the China-based executives who responded to the survey were affected by fraud, an increase from the 67% reported for China in the previous Kroll Global Fraud Report. The incidence of IP theft (12%) was the second highest of any of the countries covered (after India) and around three times the global average (4%). China also had the third highest incidence of corruption and bribery (18%), which was well above the global average (11%).

The biggest concern arises from how worried respondents in China are about fraud risks. When asked how vulnerable they believe they are to 11 different types of fraud, China ranks the highest in terms of vulnerability for nine fraud types (marked with an asterisk) among the countries covered in this report.

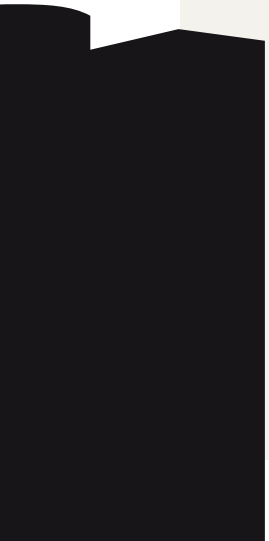
	CHINA	OVERALL
Theft of physical assets or stock*	87%	62%
Information theft, loss or attack (e.g., data theft)*	81%	51%
Corruption and bribery*	81%	40%
Vendor, supplier or procurement fraud	74%	49%
IP theft (e.g., of trade secrets), piracy or counterfeiting*	71%	37%
Internal financial fraud or theft*	69%	43%
Misappropriation of company funds*	69%	40%
Management conflict of interest*	65%	36%
Regulatory or compliance breach	65%	40%
Market collusion (e.g., price fixing)*	64%	26%
Money laundering*	63%	34%

Kroll is seeing an increase in client matters related to IP theft, information theft, corruption and bribery, and conflicts of interest in China, so it's no surprise that respondents feel vulnerable to these fraud types. Compared to figures obtained from the previous report, all these fraud types saw marked increases.

Despite these high vulnerability figures, executives in China are not investing in appropriate anti-fraud strategies. For example, 82% of respondents indicate that they are currently investing in financial controls to mitigate fraud. However, while internal controls can be useful, they must be supported with the appropriate level of employee and third party vendor due diligence, in addition to adequate compliance training and proactive data analytics to identify anomalous transactions or behaviour. According to the report, only 35% of respondents indicated that their company invests in staff due diligence, which is surprisingly low for a market which indicated that fraud is mainly an inside job (72%). Likewise only 53% of respondents indicated they invest in conducting due diligence on partners and/or vendors despite 74% feeling vulnerable to vendor, supplier or procurement fraud in China.

CHINA REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	73%	67%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Theft of physical assets or stock **(23%)** ■ Corruption and bribery **(18%)** ■ Information theft, loss or attack **(16%)**	■ Theft of physical assets or stock **(23%)** ■ Management conflict of interest **(20%)** ■ Vendor, supplier or procurement fraud **(18%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**91%**	**80%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(24%)** ■ Entry into new, riskier markets **(18%)**	■ Increased outsourcing and offshoring **(44%)**



Human trafficking and the link to fraud in supply chains

By Richard Dailly, Managing Director

Fraud can happen anywhere within a company's supply chain and affects companies in any sector. The problem is exacerbated in developing markets, where the risk of fraud and corruption may be higher and the rule of law weaker. While regular audits of vendors is increasingly accepted as a best practice in many industries, the risk of improper payments, corruption and fraud by vendors remains high. Furthermore, with a growing demand for companies to implement sustainability practices, and a parallel emergence of related regulations, it is imperative for companies to get ahead of potential ethical risks such as forced labor, land disputes and poor working conditions within their supply chain.

In the last year, numerous headlines exposed instances of forced and child labor, land disputes and poor working conditions in the supply chains of prominent global brands, particularly those in the electronics, garment and seafood industries. Conventional approaches to due diligence and compliance are often inadequate to detect these violations, especially in increasingly complex and multijurisdictional supply chains.

Navigating the myriad regulations and compliance risks within supply chains can be a daunting task for any company, one that may be perceived as too expensive, cumbersome and difficult. However, undetected noncompliance can lead to not only potentially significant financial and legal repercussions; it can also damage a company's reputation among clients, consumers and other key stakeholders. A well-designed approach to address risks throughout the life cycle of a vendor relationship, and increasing visibility into supply chains, can help companies mitigate against these risks and get ahead of potential problems.

Challenges in detecting fraud

Even companies with robust supply chain compliance practices face unexpected challenges in detecting and investigating fraud in emerging markets. The opaque nature of many of these markets and the increasingly sophisticated forms of unethical activity are difficult to trace. Common challenges companies face in addressing these risks within supply chains include:

Limited visibility – Knowing your business partner or supplier is fundamental, but in many emerging markets determining the true ownership of a company, property or factory is difficult. Obtaining reliable corporate information can be challenging in jurisdictions where records may not exist or may be unreliable. This may lead to proximity to entities that are politically exposed or sanctioned or engage in disreputable activities. Kroll investigations have uncovered instances of child labor, forced labor and undisclosed subcontracting in the supply chains of companies, including those with compliance measures in place.

Audit limitations – Many companies rely on internal or third-party audits to root out fraud and noncompliance. While regular audits are essential to identifying potential

issues, the overt approach and broad scope of audits can permit information gaps that may leave a company unaware of fraudulent activity and noncompliance. While audits can help identify compliance issues with a particular supplier, it is imperative to understand the network of third parties, such as brokers, recruitment agencies and other vendors, where violations are more likely to occur. This requires an audit strategy that goes beyond the proverbial factory walls and the first tier of suppliers.

Subcontracting – The common practice of subcontracting, often undisclosed, can hamper conventional audit and compliance efforts. Hence, standards enshrined in contracts or codes of conduct may be disregarded by subcontractors and other third-party agencies that provide services or labor to a primary vendor. This is the tier of the supply chain where fraud and labor issues, such as human trafficking, are most likely to occur. Auditing all vendors and subcontractors engaged by a company is often not a realistic or practical option; however, companies can implement a strategic approach to identify and monitor high-risk vendors to ensure compliance to contracts and codes of conduct.

Emerging regulations

The emergence of regulations aimed at addressing labor violations in supply chains is a reflection of increased pressure for companies to take a proactive stance in addressing fraud and unethical activities in their supply chains. In the United States, new regulations, such as the California Transparency in Supply Chains Act, require certain companies to disclose their efforts to identify and address human trafficking within their supply chain. Similarly, the Executive Order on Strengthening Protections Against Trafficking in Persons in Federal Contracts issued by Barack Obama in 2012 directs the amendment of federal contracting regulations to contain various prohibitions and requirements for federal contracts, subcontractors and their employees that are aimed at eliminating the potential for trafficked labor in their supply chains. Similar laws are being mooted in Europe and Asia.

Companies also need to consider the secondary risks associated with unethical and noncompliant operations within supply chains. In many cases where trafficking or forced labor has surfaced, there is an associated risk of suppliers and contractors making inappropriate payments to officials, labor agencies and other agents. These payments risk violating existing anti-bribery and anti-money laundering laws, and could even lead to complicity in inadvertently supporting criminal activity such as human trafficking.

Strategic response

Detecting fraud in supply chains requires a strategic approach that leverages available tools—such as procurement data, analytics and due diligence—and comprehensive regular audits to identify and target high-risk vendors. Conducting thorough due diligence on new vendors and a periodic review of existing ones will help develop an understanding of risks that goes beyond performance to include a sophisticated understanding of a vendor's ownership structure, connection to government officials and their relationship with subcontractors.

Kroll's ability to undertake investigations, overt and discreet, into supply chains can reveal hidden compliance and reputational issues and help you develop a comprehensive understanding of risks throughout supply chains to avoid information gaps and illuminate areas where fraud is most likely to occur.

Richard Dailly is a Managing Director for Kroll's Southeast Asia Investigations and Disputes practice, based in Singapore. With 25 years of professional experience, Richard focuses on complex business intelligence and other complex multijurisdictional cases across the region. Richard has been at the forefront of Kroll's growth in Southeast Asia, developing clients in the region and expanding Kroll's network and presence from Australia to Myanmar.

Successful internal investigations in China start with clear, compliant employee policies

By Violet Ho, Senior Managing Director and Dr. Isabelle Wan, Leader of IP and Employment Law Practices, TransAsia Lawyers

Fraud, corruption, intellectual property theft, information leaks — these activities are often traced back to employees. However, in China, if a company has not done its homework with its employment-related policies, it may find its hands tied when it comes to investigations or protecting its interests in labor disputes.

Kroll Senior Managing Director Violet Ho and Dr. Isabelle Wan, leader of the IP and Employment Law practices with TransAsia Lawyers, have written a white paper discussing issues that they have encountered across numerous cases and the strategies employers can take to better position themselves in the event of employee-related fraud in China. This article presents highlights from that paper.

Lay a strong foundation with detailed employee record-keeping

In our experience, we have found organizations operating in China with woefully inadequate HR record-keeping. Take something as basic as an employee's name. Chinese employees who work for multinationals often use an English name for communicating with colleagues and clients. And yet, this is usually the only name on file in employment records. This makes it extraordinarily difficult to conduct an investigation when a person's true identity isn't known.

So, the first step must be to create employee registration records that capture detailed identifying information, to include legal names, aliases, ID numbers, addresses, contact information, etc., including data for family members.

Because there is currently no comprehensive body of laws in China setting out a detailed, uniform set of rules on the collection, processing and use of personal information, employers are advised to outline in their employee handbooks or in a separate letter (which must be signed by each employee personally and retained by employers) that employees agree to:

- disclose their personal data to the employers
- authorize their employers to use and retain such personal data within a specific permitted scope of use agreed upon by both parties. Such purpose could extend to investigation for employee misconduct

Produce and distribute a comprehensive employee handbook

The importance of a properly drafted, comprehensive and legally compliant employee handbook cannot be overstated when operating in China, where it is normal for both employers and employees to grapple with their rights and obligations in an employment relationship.

Consider this actual case: A general manager was dismissed for withdrawing a large sum of money from his employer's bank account. Before leaving, he took with him the company's official seal and all corporate documents. He then proceeded to forge an employment contract, adding more benefits for himself (totaling more than $1.6 million), and then initiated a labor dispute arbitration case against the company for wrongful dismissal, claiming the benefits under his forged contract. As the company's handbook was unclear on the reimbursement policies, cash withdrawal process, authorization procedures, proper use and management of the company's official seal, and contract signing procedures—as well as the corresponding punishment—the company was unable to rely on them to terminate the fraudster for his misconduct and misappropriation of company property.

When creating an employee handbook for use in China, employers should keep in mind the following:

- There is a difference between an employment contract and an employee handbook. For example, since non-compete agreements are post-contractual obligations, they must be stipulated in the employment contract or in an independent non-compete agreement, not in an employee handbook

- The handbook must be prepared in Chinese (indeed, all employment-related documents should be in Chinese) and publicized to employees. If there are any discrepancies between the English and Chinese language versions of an employment document, the Chinese language version will always prevail under the law
- Likewise, companies operating in China need to customize their policies to ensure compliance with not only PRC national law, but also with local rules and judicial practices. Companies should work with experienced local counsel to review all forms and policies and ensure that potential conflicts do not exist that could impact enforcement
- The handbook must be distributed to employees in a hardcopy version, and the company must ensure that an acknowledgement of receipt is executed by each employee in person
- The handbook must set out in detail the internal rules and policies of the company. Failure to include relevant content or conversely, the inclusion of invalid or illegal content in the handbook will put the employer at the losing end of any labor dispute case
- The handbook must also include specific provisions relating to the discipline of employees and the punishment corresponding to each type of misconduct. The employee handbook is a key document in labor disputes because it can prove that the employee had notice of the consequences of his/her misconduct, and that the severity of the punishment was explicitly proportionate to the violation

To aid in potential internal investigations, two critical policies should feature prominently in the employee handbook: Information Technology (IT) Policy and a Social Media Policy.

- The IT policy should clearly state that employees agree (i) they will have no expectations of privacy when using the company's IT resources and communication systems; and (ii) the company has the right to monitor the use of its IT resources and communication systems—including any activity on personal email accounts accessed on company computers—to ensure compliance with the policy
- Many Chinese routinely use Twitter and its Chinese counterpart, Weibo, to conduct personal business. Companies should impose a specific social media policy spelling out what employees cannot share about the company's business operations on their social media accounts and outline disciplinary actions if violated

Current events make this a good time to review employee data access policies

On March 15, 2015, the evolution of data privacy protection in China reached a milestone as the "Measures for Punishments Against Infringements on Consumer Rights and Interests" went into effect. These Measures provide criteria for the first time as to what constitutes personal information under Chinese law.

While the Measures do not provide specific guidance for employers, now is a good time for companies to evaluate where they stand in regards to employee data access policies. However, the approach must be considered and measured, and applied on an even keel. Otherwise, employees might raise accusations of discrimination if they perceive to be targeted. Alternately, too narrow a focus could tip off people that something is amiss. A better strategy is to make it a company-wide exercise that involves the entire employee population.

Violet Ho is a Senior Managing Director for Kroll's Greater China Investigation and Disputes practice. With over 16 years of professional experience in investigations, and an in-depth understanding of China's business environment, Violet has successfully advised on numerous highly complex investigative projects in China and beyond.

Dr. Isabelle Wan is leader of the Employment Law practice and co-leader of the Intellectual Property Law practice with TransAsia Lawyers. Wan has 24 years of experience in advising clients on foreign direct investments in China. She is the first non-PRC national to serve as a Director of the China Labor Law Studies Association and is generally considered by relevant government agencies as the leading practitioner for employment and social security.

India overview

India has one of the largest fraud problems of any of the countries covered in this report. Its 80% overall prevalence is third in this group compared to Colombia's 83% and Sub-Saharan Africa's 84%. It also has the highest national incidence of corruption (25% of companies), regulatory breach (20%) and IP theft (15%). It also ties for the highest national level of money laundering (8%). The outlook for the future is also worrying: 92% of Indian respondents reported that their firms had seen exposure to fraud increase in the past year.

For every fraud covered in the survey, respondents from India are more likely than average to report that their firms are highly or moderately vulnerable. In particular, they have the highest proportion reporting this level of exposure to vendor or procurement fraud (77%), corruption and bribery (73%) and regulatory or compliance breach (67%).

While companies in India are willing to spend to improve their level of anti-fraud protection, it appears that such funds are not being invested appropriately. For respondents that had identified the perpetrator, 59% indicated that junior employees were leading players in at least one such crime. Despite these vulnerabilities and the high proportion of fraud perpetrated by insiders, only 28% of companies in India invest in staff background screening and only 55% invest in vendor due diligence. Greater attention to employees and reputation-focused due diligence might significantly bolster other fraud efforts at firms in India.

INDIA REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	80%	69%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Corruption and bribery **(25%)** ■ Vendor, supplier or procurement fraud **(23%)** ■ Regulatory or compliance breach **(20%)**	■ Theft of physical assets or stock **(33%)** ■ Information theft, loss or attack **(24%)** ■ Corruption and bribery **(24%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**92%**	**71%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(28%)** ■ Cost restraint over pay **(21%)**	■ IT complexity **(33%)**

Investing and operating in India: Getting the most out of your private equity investment

By Reshmi Khurana, Managing Director

By some estimates, over $500 million worth of private equity (PE) investments in India are embroiled in legal disputes.[1] Kroll's experience in the country suggests that disputes in the legal domain represent only a small fraction of the actual number of situations where investors are in serious disagreement with the owners or management of the investee companies. In our work supporting PE investors in such disputes, even the most seasoned PE investors who understand the Indian business environment have executed deals where they are unable to maximize the potential of their investments due, in part, to a dispute with the portfolio company.

Reshmi Khurana, Managing Director and head of Kroll in India, explains the various investigative tools available to PE investors that can help them minimize potential losses post acquisition should such disputes arise.

Q – What are the various circumstances in which PE investors in India may enter into disputes with a portfolio company?

Most disputes are triggered when PE investors suspect fraud in a portfolio company. The majority of deals in India are minority investments where promoters continue to control the business and the flow of financial information after a PE investment. Additionally, corporate governance standards in India are still evolving, especially in regards to small and mid-sized companies. As a result, promoters may be following certain business practices which may not necessarily be aligned with the interests of the PE investor, such as related party transactions and diversion of funds for other businesses. In such situations, it becomes difficult for a minority PE investor to understand the true performance of the portfolio company.

PE investors should be alert to these tell-tale signs of potential fraud:

- Performance of the portfolio company starts deteriorating shortly after the PE investment is completed
- Funds from the PE investor are not used in the manner that was agreed to prior to the investment
- PE investor is denied access to good quality financial information and to the management of the portfolio company

Disputes between PE investors and promoters can also arise due to differences in valuation practices (with respect to shares) and shareholder rights as well as exit options. Indian promoters have been relatively slow in delivering exit options to PE investors over the last few years, and PE investors in India often own companies for five, seven or even 10 years. This has impacted their returns and leads to the potential for further disputes.

Q – Given these difficulties, what should PE investors do to mitigate or avoid such potential disputes with promoters of portfolio companies?

While investigating fraud in portfolio companies, we see that the greatest erosion of value in a portfolio company occurs within the first 18 to 24 months of the PE fund's making the investment. Whether promoters are diverting funds out of the company (through illegal cash kickbacks from vendors) or manipulating financial data, our experience suggests that fraud occurs soon after the investment.

While a forensic review of the financial data of an investment target can identify red flags, it cannot necessarily be relied upon to uncover fraud. In Kroll's experience, perpetrators often cover their tracks with false documentation and transactions that appear genuine and do not raise alarms in the pre-investment review. PE investors can avoid surprises and disputes by conducting in-depth and independent due diligence on the target company. This means fully investigating red flags or other symptoms of poor performance that are identified pre-investment. They should select due diligence providers on a "no compromise basis" to ensure that such providers are truly independent and the integrity of the due diligence process is maintained.

Most PE funds embed management information systems (MIS) and other business intelligence systems immediately after the investment is completed. We believe this is not enough to quickly identify and root out problematic areas that could erode the potential value of the investment. Investors should take an active and investigative approach to understanding the true business practices and controls in the portfolio company and use various fraud prevention tools to ensure their interests are protected.

Q – If a PE investor does suspect fraud in a portfolio company in India, what should it do?

Usually the first thing a PE investor wants to find out in such a situation is what is going on in the portfolio company. The PE investor's ability to answer this question depends on its access to the financial information and management of the portfolio company. As mentioned above, because most PE deals in India are minority investments, typically the only access to financial information that PE investors have is through monthly MIS reports, which may not represent or give an accurate picture of the true performance and practices of the company. Additionally, PE investors in India do not like to challenge promoters in court early on because of the generally slow pace of the judicial system in India.[2]

In these circumstances a PE investor can conduct a discreet, "outside-in" external investigation of the portfolio company. This can provide useful indications of poor business practices or malfeasance on the part of the company; the promoter's reputation in the market as well as their conflicts and assets; and whether the promoter or management are known to be involved in fraudulent practices and if so, what these practices are. PE investors often use the information gained through this exercise to negotiate with the promoter to gain greater access to the financial data of the company before the deal is done.

Q – Where should PE investors focus if they obtain access to financial data?

In some instances when some or all of the company's financial data is available, the PE investor can conduct a full forensic audit of the company's operations. The review can be conducted onsite or offsite and may include access to the company's ERP systems and management. The typical areas of focus include understanding the gap between book profits and cash profits, capex overload, revenue recognition methods, and review of policies, SOPs, filings, etc.

Q – Do these findings constitute evidence in India and how can this information be leveraged effectively?

First, the bar is set high for what constitutes evidence of fraud in a court of law in India; second, once in court, it can take years to settle disputes, by which time the value of the investment may have significantly eroded.

These factors explain why PE investors are usually not keen to go to court immediately following a dispute. That said, there are various ways that PE investors in India have used the information gathered during the investigation to overcome the challenges of the existing legal framework. They can use the information to negotiate with the promoter, up to and including the threat of naming and shaming. And of course, sometimes the information can be used to take a successful court action.

Q – How do you see the corporate governance environment in India evolving in the future?

Corporate governance in India is evolving in a positive way, and this is being led by a new generation of entrepreneurs. They have experienced the many benefits of following sound corporate governance practices, from being rewarded by investors to seeing firsthand how transparency in their financial reporting helps them make the right business decisions.

The question is, once these businesses grow to a particular size and scale, will these entrepreneurs and the corporate governance foundation they are establishing be able to withstand the external pressures that often accompany growth?

[1] http://www.livemint.com/Companies/r2zRRIAnYAfGSazpLRKqcO/Over-3000-crore-PE-investments-stuck-in-legal-battles.html
[2] http://www.ft.com/intl/cms/s/0/6c2e72fc-6c03-11e4-b939-00144feabdc0.html#axzz3XMxM7PBc

Reshmi Khurana is a Managing Director and head of Kroll's India office. Reshmi has more than 15 years of experience conducting complex corruption investigations, litigation support and due diligence on the management, operations and business models of organizations across the U.S., South Asia and Southeast Asia. Her clients include asset management companies, corporations in the mining, oil and gas, consumer packaged goods and pharmaceutical industries, and law firms.

Europe overview

Despite the widespread assumption that Europe experiences relatively low levels of fraud compared to other regions, 74% of European respondents suffered at least one type of fraud in the last 12 months, close to the global level of 75%. Europe also has the highest regional rate for two frauds: theft of physical assets (27%) and regulatory and compliance breach (15%). In fact for seven of the 11 frauds covered in the survey, European respondents reported an above-average incidence.

However, Europeans are less likely than average to believe that their firms are highly or moderately vulnerable to fraud. One exception is regulatory and compliance breach, where 41% of European companies felt highly or moderately vulnerable, compared to 40% globally. Europe's incidence of this fraud was reported to be one quarter higher than the global mean (15% compared to 12%).

Insider malfeasance is another area of concern for Europe. Respondents are the most likely from any region to report that high staff turnover increased fraud exposure (39%) in the last year. Similarly, when their company has suffered at least one fraud and the perpetrators are known, they have the highest number reporting that junior employees played a leading role (46%). Nevertheless, respondents are less likely than average to say that they are investing in staff background checks in the coming 12 months (33% compared to 37%).

EUROPE REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	74%	73%
LOSS Average percentage of revenue lost to fraud	0.8%	1.2%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Theft of physical assets or stock **(27%)** ■ Vendor, supplier or procurement fraud **(18%)** ■ Information theft, loss or attack **(16%)**	■ Theft of physical assets or stock **(28%)** ■ Vendor, supplier or procurement fraud **(25%)** ■ Information theft, loss or attack **(21%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**75%**	**77%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(39%)** ■ Increased outsourcing and offshoring **(19%)**	■ IT complexity **(37%)**

Operate globally? Investigate locally.

By Marianna Vintiadis, Managing Director

As the world economy becomes more integrated, investigations are rarely limited to a single jurisdiction. But the world is not only more integrated, it is also more regulated, forcing investigators and their clients to take account of local differences.

Few activities are as intimately connected to territory as investigations. Even the nature and availability of publicly available information varies by jurisdiction, making local knowledge crucial. In Italy, for example, transfers of residence must be declared to the authorities, who then check the information and place it in a publicly accessible register. In Greece, on the other hand, no such register exists. So, in certain places ascertaining an individual's residence is a very simple matter; in others, the same exercise may require a complex investigation.

As countries respond to the drive for open and transparent government, the nature of what data are available and how to access them changes, requiring further location-specific skills. More important still, though, is interpretation: here a deep understanding of norms, conventions and references can make all the difference. "They made him an offer he could not refuse" is a simple example: the turn of phrase might refer to a great employment prospect, but in an investigation into organized crime it acquires ominous connotations. Anyone who has read intercept transcripts, for example in the context of a litigation support assignment where evidence is made available by the prosecutor, realizes that understanding relevant industry slang and background information and context is key to accurate interpretation.

Similar considerations apply to whistleblower letters. Poor grammar or lack of clarity could lead to dismissal of a serious allegation simply because it is misunderstood, but familiarity with a local expression, for example, may help determine the location where a fraud is taking place. This is especially important when looking at complaints from poorly educated whistleblowers who, more often than not, take an understanding of the context of their complaint for granted and thus send cryptic notes.

Even understanding and contextualizing press articles in certain countries requires knowledge beyond simple linguistic skills. At a basic level, is a given local journal independent or is it the mouthpiece of a particular owner or a political party? The problems do not end there: even an allegation in a respected, mainstream, high circulation publication may require context. If an Italian newspaper, for example, writes that someone has been "placed under investigation," it may not mean much. In Italy, the law requires that any crime report—for example, a complaint filed with the police—however improbable, must spark an investigation.

Once we go beyond public sources, the importance of local knowledge only grows. It is essential in planning a successful inquiry. Are people likely to talk? What might be the most effective way to approach them? Going back to organized crime, in certain countries simply knocking on neighbors' doors in search of testimony is likely to lead to only one outcome… omertà.

The nuances of communication are not the only local consideration. Regulation determines what any investigator can or cannot do in each territory. Some countries require licenses; others do not. Some regulate surveillance; many ban it outright; others still do not regulate it at all. The same applies to any investigative activity, from collecting press clippings – surprisingly, even this is illegal in some places – to rummaging through rubbish.

Take, for example, a pre-employment background check or an email review in the context of an internal investigation. The relevant rules and regulations vary dramatically by country. Even within the European Union, local versions of privacy or employment law can affect an investigator's options dramatically. Pre-employment checks require informing the subject in advance in most European countries. Access to email is heavily regulated, whether or not corporate computer use policies alert employees that such communications can be accessed in case of an investigation. Indeed, although the government is reviewing this provision at the moment, at the time of writing in Italy, even in cases of fraud or serious misconduct, companies need to alert an employee in advance, in writing, of a specific investigation.

Different regulatory environments affect internal compliance programs as well. A multinational's anti-corruption program might meet local legal requirements at headquarters, but there is no guarantee that subsidiaries abroad are adequately covered. One way of approaching the problem is to consider the tools at one's disposal at each local level and work backwards to construct a robust policy that will not only ensure compliance but also provide adequate means of efficiently limiting damage if a problem actually arises.

Even in our globalized world, then, companies need to be aware of national differences. Upon receipt of a whistleblower allegation, prior to hastily accessing someone's email account in Latvia, Greece or Portugal, even if the corporate server is sitting comfortably in Texas, find an expert who can guide you through the local language as well as social and regulatory nuances.

Marianna Vintiadis is Kroll's Country Manager in Italy and is also responsible for Kroll's operations in Austria and Greece. Since taking over Kroll's Italian office, Marianna has successfully developed Kroll's local client base which today includes the country's largest corporations and financial institutions as well as its leading law firms. She has also opened Kroll's services to the Italian SME market, which forms the backbone of the Italian economy.

Sub-Saharan Africa overview

Sub-Saharan Africa has for many years been the region with the largest fraud burden, and this has not changed. It has the highest proportion of companies affected by at least one fraud (84% compared to a survey average of 75%). It also had one of the highest average losses to fraud in the last 12 months (1.0% of revenue) of any region.

Things appear to have improved, however, in the incidence of individual frauds. In common with much of the world, most of these have fallen. Nevertheless, Sub-Saharan Africa still has the highest regional rate of vendor, supplier and procurement fraud (22%) which remains little changed from the level in the previous survey (23%).

More worrying than the high incidence of fraud in the region, though, is that executives seem to have become inured to the problem. For every fraud in the survey, respondents from Sub-Saharan Africa are less likely than average to see themselves as moderately or highly vulnerable. Indeed, for internal financial fraud and misappropriation of company funds they are the least likely to see themselves as vulnerable to this extent, even though the incidence of both frauds in the region was above the global average.

At the same time, those from the region are engaging in riskier behavior. Sub-Saharan Africa has the second highest regional figure for increased fraud exposure in the last year. It also has the highest number of respondents for any region reporting increased risk from entry into new markets (22%) and from increased outsourcing and offshoring (22%) – flip sides of the region's extensive economic growth.

Perhaps because of low risk perceptions, Sub-Saharan Africans are not active on fraud in general, but instead are closely focused on two specific defenses. Respondents in the region are the most likely to report increased investment in physical asset and information security measures, but are less likely than average to be putting money into every other defense covered in the survey. Fraud levels remain so high that a more holistic approach is needed.

SUB-SAHARAN AFRICA REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	84%	77%
LOSS Average percentage of revenue lost to fraud	1.0%	2.4%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Theft of physical assets or stock **(24%)** ■ Vendor, supplier or procurement fraud **(22%)** ■ Corruption and bribery **(14%)** ■ Misappropriation of company funds **(14%)**	■ Theft of physical assets or stock **(47%)** ■ Corruption and bribery **(30%)** ■ Internal financial fraud or theft **(27%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**86%**	**86%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(35%)** ■ Entry into new markets **(22%)** ■ Increased outsourcing and offshoring **(22%)**	■ IT complexity **(48%)**

African natural resources: Economic trends and fraud risks

By Alexander Booth, Senior Director

Short term challenges, strong fundamentals

Africa's wealthiest Forbes-listed tycoon lost $4.4 billion in a little over a month toward the end of 2014. He was not alone. Several of Nigeria's largest listed companies have seen their market capitalization shrink dramatically over the last year due to a combination of local and global macro-economic factors. These include the devaluation of the naira, which has erased tens of billions of dollars from the value of the country's economy.

Other countries across the continent with economies closely tied to commodity prices are also experiencing pain. Following a 47% drop in the price of iron ore in 2014, South Africa's largest producer announced in February plans for job cuts and reduced capital expenditure. In Zambia, the sliding copper price has caused the kwacha to depreciate to record lows against the dollar. Several mining companies in that country are considering cutbacks.

In the oil and gas sector, businesses providing services to larger exploration and production operators have already come under immense pressure to narrow their profit margins. Many projects which have not yet entered production may be mothballed as the majors shore up capital and independent firms can no longer afford the risk of exploration in frontier markets. Some large-scale job cuts have already occurred.

However bleak the current picture, though, in the eyes of many investors, African natural resources remain an attractive prospect in the medium- to long-term. Projects in advanced stages or where a significant amount of capital has already been committed are likely to continue. Furthermore, opportunities exist for savvy buyers with strong balance sheets to pick up assets at a discount, directly or through mergers and acquisitions.

Political and governance risks

Which risks do those buyers need to be aware of? Kroll has seen that the current complex and rapidly evolving economic landscape may have serious implications for corporate and public governance in the African natural resources sector. This in turn is affecting how our clients need to evaluate their routes to market, raise funds and scrutinize their existing portfolios of businesses across the continent.

One area of potential concern is increased uncertainty in political decision-making driven by a packed political calendar. By the close of 2015, many African countries – among them key markets such as Nigeria, Ethiopia, Guinea and Cote d'Ivoire – will have seen parliamentary and presidential elections take place. As a result, long-standing political fault lines may be disrupted, with substantial implications for the private sector in a region where the gap between business and politics is often indiscernible.

At the same time, officials are contending with an increasingly demanding electorate. In almost every country, governments are coming under mounting pressure to extract more value from natural resources for the local population, whether through increased revenue for state coffers or enhanced local content laws. The result is a credible fear that perceived "resource nationalism" is likely to deter foreign investment at a time when low commodities prices and devaluating currencies are leading to bloated budget deficits.

These factors have led to erratic or reactive decision-making in some cases, causing uncertainty for local and international investors. For example, in 2014 the majority of mining companies operating in Zambia paid next to no income tax, citing a failure to turn a profit due to poor market conditions. However, the government—under increased pressure to raise revenue—accused mining companies of tax evasion. It controversially scrapped corporate tax but increased mineral royalties from 6% to 20%. This resulted in widespread protests and several operators threatened to close down. In January 2015, Zambian elections ushered in a new administration which ultimately reversed the contentious mining tax policy, but investor confidence will take time to recover.

Apart from political uncertainty, the challenging economic environment also increases the risk that players across the natural resources sector will be tempted to cut corners in order to unplug bottlenecks, recoup costs on existing

projects or secure project finance. This in turn significantly heightens the risk of encountering fraud and corporate malfeasance.

Quality intelligence is critical to pre-empting the risks

Two examples drawn from a wide range of intelligence gathering and investigative assignments conducted by Kroll in recent months illustrate some of the more common risks.

With market capitalization shrinking and cash flow under pressure, smaller listed mining companies – particularly those pursuing a single mineral play or in regions affected by Ebola – have been under severe financing pressure. Some management teams have looked to unorthodox sources of funding that they would not consider in a more stable economic environment. In one case, Kroll was retained to investigate the background and probity of two young Angolans, who had offered to inject several hundred million dollars into our client's mining operations. Our research centered on the identity of the potential investors, the provenance of their wealth and their connections to the Angolan political elite. We identified several areas of concern—in some cases a question of what was absent rather than what was present. First, the two individuals had no discernible track record in the sector and had never been involved in securing financing for projects of this scale. Despite thorough and widespread inquiries in Luanda, we were unable to identify anyone who could vouch for their reputation. Moreover, our investigation revealed serious doubts about the credibility and legitimacy of the individuals' source of funding. We found information to suggest that they could be acting as "fronts" for unknown actors, potentially politically exposed persons or government officials through a series of offshore vehicles and accounts. Ultimately, the client, against its initial hopes, chose to decline the funding package.

How funds are—or are not—being used can be just as problematic as their source. Recently, an international mining and metals group asked Kroll to investigate progress at an African mine site in which it had invested. Since putting in its money, our client had received minimal communication from the project developer, not been invited to participate in decision-making on the mine's operations and been blocked from accessing the site (in breach of its agreement with the developer). Kroll drew on its regional knowledge and portfolio of well-placed local contacts to assess progress of the project and gather live intelligence on the project developer's activities and intentions. We learned that the developer had missed certain deadlines and performance benchmarks imposed by the host government, was under immense funding pressure and was discreetly seeking to raise fresh equity which would have resulted in a material dilution of our client's stake in the mine. Our evidence informed the client's tactical response to the problem and was also shared with their external legal counsel in support of litigation against the project developer.

Investments in natural resources give rise to particular risks because of the scale and longevity of financial commitments, and the need to interface closely with government regarding licenses, permits and taxes. Furthermore, fraud and corporate malfeasance are not always identified by traditional legal and financial due diligence. Our recent work in Africa has uncovered many types of fraud ranging from regulatory and compliance breaches, through to conflicts of interest and vendor, supplier and procurement fraud. It is only by fully understanding how and when these issues occur across the continent that investors can accurately gauge the risk, increase the chance of controlling it and create a stronger framework for realizing a return on their investment in a challenging investment climate.

Alexander Booth is a Senior Director specializing in complex business intelligence assignments and emerging markets including Africa and the Middle East. Alexander has been involved in a diverse range of cases, and developed particular expertise in managing networks of sources in sensitive environments, particularly in DRC, Nigeria, Ghana and Angola.

Russia overview

The overall prevalence of fraud which Russian respondents reported this year remains at much the same level as in past surveys. Moreover, although as in much of the world the incidence of many specific frauds has dropped, Russia still saw the highest national incidence of misappropriation of company funds (17%) of any of the countries discussed in the Global Fraud Report.

Corruption also remains a significant problem, with 20% saying they were affected—the second highest figure among the countries. Part of the problem is the environment. Half of Russian respondents say that their firms are highly or moderately vulnerable to this crime. Moreover, where any fraud has occurred and companies know the perpetrators, 9% of Russian respondents report that a government official was involved, by some margin the highest figure in the survey.

Looking ahead, two things suggest that the fraud situation might get worse. First, nine out of 10 Russian respondents reported that their fraud exposure had increased, including 43% who said that high staff turnover contributed to this—the latter being the highest figure for any of the countries reported on from the survey. On the other hand, the proportion of Russians saying that their firms will be spending on fraud defenses which might reduce corruption or employee-based risk—management controls, staff background checks and staff training—are all below the survey average. This may prove to be an unfortunate combination.

RUSSIA REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	73%	76%
LOSS Average percentage of revenue lost to fraud	0.5%	1.9%
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Theft of physical assets or stock **(20%)** ■ Corruption and bribery **(20%)** ■ Misappropriation of company funds **(17%)**	■ Corruption and bribery **(32%)** ■ Information theft, loss or attack **(29%)** ■ Management conflict of interest **(24%)**
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**90%**	**74%**
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(43%)** ■ Entry into new, riskier markets **(10%)**	■ IT complexity **(35%)**

Business as usual in Russia, despite political headwinds

By Alessandro Volcic, Associate Managing Director

Surprising economic resilience

Rumors of the death of the Russian economy appear to be greatly exaggerated. Discussion of the investment climate for much of the last year has tended to focus on large, negative developments, in particular: the imposition of sanctions over the conflict in Ukraine; a precipitous drop in world crude oil prices; and a corresponding decline in the value of the ruble. These have certainly had a collective impact. Economic growth overall was largely flat last year, and the consensus is that some decline will occur this year.

On the other hand, recent news is much more positive. Slowly rising oil prices have brought both modest recovery in the value of the ruble as well as a renewed sense of cautious optimism that the worst is over. Some forecasters still expect 2015 to be a year of recession – with GDP expected to fall from anywhere between 2% and 4% depending on who does the analysis – but many have been reducing their predictions of the extent of the drop. Most also see a return to growth in 2016.

Moreover, as with any mild downturn, there are winners as well as losers. Those most affected by both sanctions and declining commodity prices have been in the oil and defense sectors. On the other hand, a cheaper ruble and Russian counter-sanctions have together bolstered local manufacturing and agribusiness industries as import substituters seek local suppliers.

Just as important, unlike in earlier downturns, foreign companies are staying put rather than fleeing from a perceived crisis. Firms such as Nestlé, Burger King and Ikea have reiterated their commitment to this market. In short, although economic conditions in Russia are currently difficult, they are within the normal ebb and flow of the ordinary business cycle.

Fraud remains a common problem...

Economic conditions indicate that companies are engaged, for the most part, in business as usual. What we have been finding is that this is also the case for fraudsters.

Fraud remains a widespread issue in Russia. According to the latest survey conducted by the Economist Intelligence Unit for this year's Global Fraud Report, 73% of firms discovered that they were victims of at least one fraud in the past year. Rather than expecting improvement, though, nine out of 10 Russian respondents to the survey reported that their firms became even more exposed to this threat over the past 12 months.

Corruption is an important part of the problem: over the years Russian respondents in our surveys have frequently reported some of the highest incidences of this crime of any country. This year is no exception, with one in five saying it had affected their businesses in the last year—the second highest figure among the countries surveyed in depth. Such findings are consistent with other data: for example, Russia finished 136 out of 175 in last year's Transparency International Corruption Perceptions Index.

...And a team game

Beyond corruption, though, our surveys frequently throw up a range of different fraud problems. This year, for example, Russians reported the highest level of misappropriation of company funds (17%), whereas in the previous survey there were above-average figures for management conflict of interest (24%) and internal financial fraud (18%).

The problem is not that the form of fraud varies widely over time in Russia. Instead, the difficulty is that any one description may not fully encompass the most common type of malfeasance that we see in our investigations. In Russia, directly embezzling funds from a firm, especially a subsidiary, is actually fairly difficult. Rather, what we often see are local managers of multinational companies who work with suppliers or other outsiders to siphon off company funds.

In one typical case, for example, Kroll was approached by a Western telecoms firm which had received allegations of wrongdoing by senior management at its local Russian operating company. The effort began small—with an email review—but what we uncovered led to an investigation which needed to include over 60 interviews with staff, suppliers and clients, a forensic accounting exercise and external inquiries. In this instance, suppliers and managers were working together to inflate prices of services and jointly pocket the difference. As a result, the firm dismissed three of its senior managers and overhauled its local compliance procedures.

Management's external collaborators are not necessarily suppliers. In another case, a well-known Western medical equipment manufacturer was concerned about links between its local management and key distributors. Kroll found that they were right to be: the Russian general director and certain other local senior executives were all involved in tainted transactions and had directly set up a number of the distributors themselves.

Finally, white collar fraudsters in Russia are also willing to use a range of partners in crime simultaneously. Recently, Kroll investigated the local management of a Nordic real estate investment fund, which engaged us to look for evidence of suspected wrongdoing and to confirm its estimated losses. We identified colluded transactions between former management and tenants, suppliers and service providers. Former management had evidently not acted in the best interest of the fund, instead taking opportunities to deflect cash out of the company. The evidence we found has since been supporting a civil recovery strategy.

Looking ahead

Predictions about the economy are not always accurate, and Russia's has its share of risks. A worsening of the situation in Ukraine and more extensive sanctions could spell trouble for the apparent incipient recovery. Nevertheless, those operating in the country are well advised not to be distracted by very real existing risks through fear of potential ones.

Among the former is fraud, in particular Russia's particular form of white collar crime. Understanding the relationships between local managers and those interacting with the company in various ways is essential to combating this risk which is far more consistent than the ebb and flow of economics.

Alessandro Volcic, Associate Managing Director, runs Kroll in Russia and the CIS and heads up the Moscow office of the firm. He has led complex international fraud investigations, internal investigations and investigations into potential Foreign Corrupt Practices Act breaches. Alessandro also oversees Kroll's due diligence offering in the region. He has conducted cases in Germany, the former Soviet Union and the Middle East.

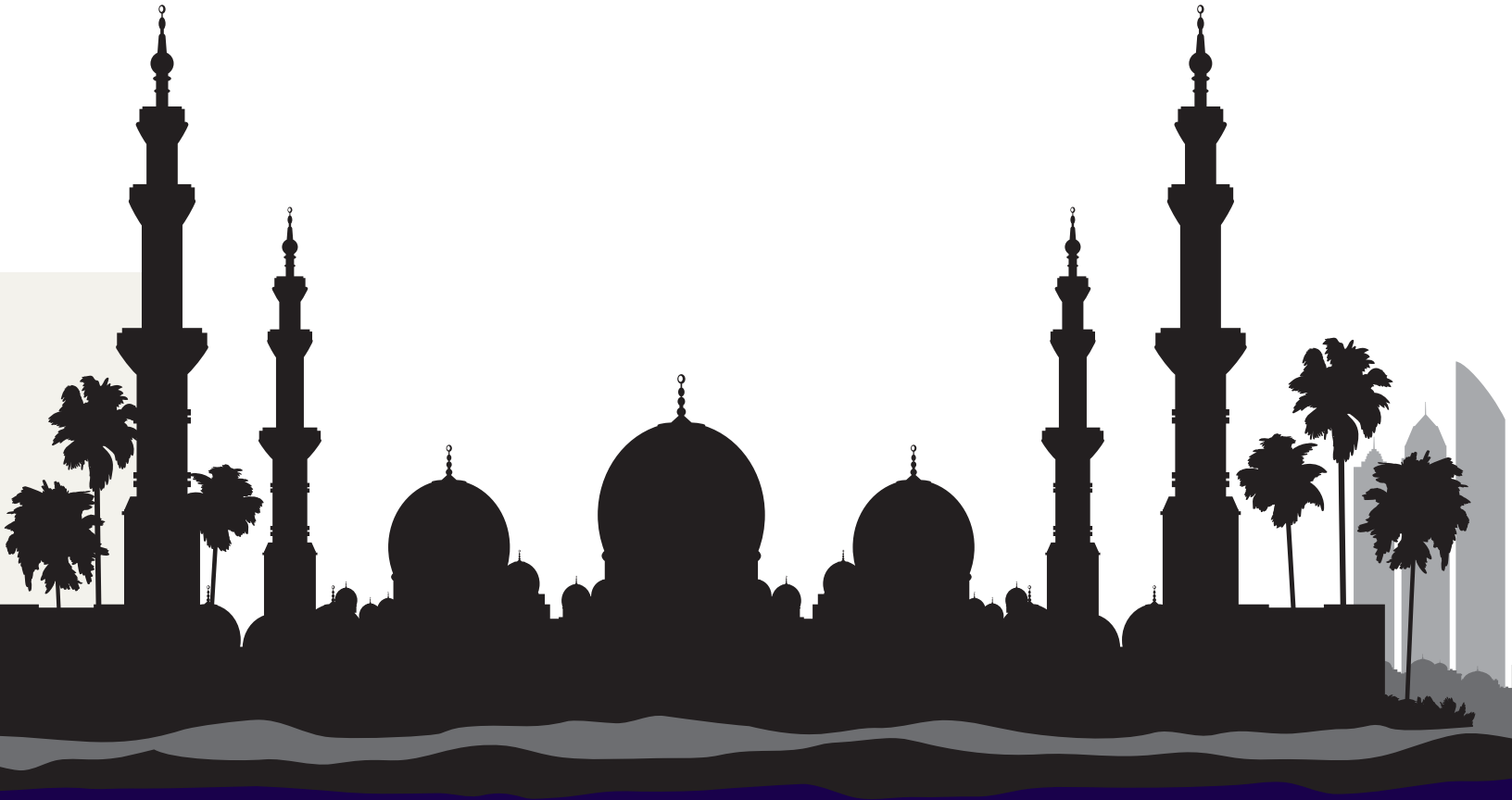
Gulf States overview

The Gulf is a generally low fraud location, although a number of notable problems do stand out. It has the lowest overall prevalence (62%) of the regions reported on in this study. Moreover, for seven of the 11 specific frauds covered in the survey, the incidence is below the survey average and for two others only very slightly above.

On the other hand, among regions covered in the survey, the Gulf has the highest regional incidence of money laundering (8%) and misappropriation of company funds (15%).

Overall, the biggest concern about the area revealed in the survey is the rate of senior and middle management malfeasance. Where a fraud has been discovered and the perpetrator known, 46% of Gulf-based respondents report that such a high-level executive was involved, well above the overall average of 36%. This in turn affects the economic impact of fraud. Previous surveys have shown that senior management crime tends to be the most expensive and, despite the Gulf's low overall fraud incidence, the average rate of loss in the country, 0.9% of revenues, was above the survey mean.

Businesses in the region are taking steps. Half of respondents report that their firms are putting money into further management controls, the highest regional figure and well above the survey average (39%). Given the survey findings, this seems a wise investment.



GULF STATES REPORT CARD

	2015-2016	2013-2014
PREVALENCE Companies affected by fraud	62%	–
LOSS Average percentage of revenue lost to fraud	0.9%	–
AREAS OF FREQUENT LOSS Percentage of firms reporting loss to this type of fraud	■ Vendor, supplier or procurement fraud **(18%)** ■ Misappropriation of company funds **(15%)** ■ Theft of physical assets or stock **(13%)** ■ Management conflict of interest **(13%)**	–
INCREASE IN EXPOSURE Companies where exposure to fraud has increased	**82%**	–
BIGGEST DRIVERS OF INCREASED EXPOSURE Most widespread factor leading to greater fraud exposure and percentage of firms affected	■ High staff turnover **(36%)** ■ Increased outsourcing and offshoring **(21%)**	–

Whistleblowers in the Gulf: Proceed with caution

By Yaser Dajani, Managing Director

Who commits fraud in the Gulf? The answer from respondents to the survey conducted by the Economist Intelligence Unit for this Global Fraud Report may be an uncomfortable one—especially in a region where even large firms are often privately controlled, usually by members of the same family. The survey found that, where a company based in the region has uncovered a fraud in the last year and the perpetrator is known, in 42% of cases a C-level executive or middle manager took a leading role in the crime's design and execution. This is the highest such figure for any region: it was 30% in the Asia-Pacific region, 35% in Europe and 39% in North America. If you take into consideration those crimes where junior employees were involved, the number of cases of fraud in the Gulf jumps to 63%.

Respondents to the survey in the Gulf do not expect this will change. High staff turnover was the most frequently cited cause of increased exposure to fraud in the region, mentioned by 36%. Despite the high employee turnover, two-thirds of all fraud that companies in the Gulf discover are committed by individuals who understand the vulnerabilities of the business and are therefore capable of manipulating operational and security weaknesses to their advantage.

So while employees can represent a fraud risk, employees are also key assets in a robust anti-fraud system. In the Gulf, however, many organizations at the shareholder and board levels fail to recognize that their employees are their most effective first line of defense. According to our survey, fraud in the region comes to light most often through an internal audit (in 44% of cases where a fraud was found). In only 20% of cases is the discovery due to a whistleblower's report. The opposite should be true. In fact, the proportion of frauds unmasked by a whistleblower in the Gulf is lower than that of any other region in the world. The global average is 41% and is as high as 48% in America, where more than 50% of whistle-blower reporting comes from employees.

This low level of employee reporting in the Gulf is driven by two main factors: first, the absence of corporate systems to report wrongdoing; and second, the lack of federal laws to protect private-sector whistleblowers, particularly if their identities are discovered and they become involved – with or without their consent – in investigations. In other parts of the world, whistleblowers are often legally protected and and may even be rewarded for the disclosure of information that leads to prosecution. In the Gulf, the situation is starkly different. Kroll has worked on cases in which whistleblowers are harassed, threatened, penalized and, in some cases, have their employment terminated. Unsurprisingly, such treatment discourages disclosure of information to either employers or regulators, even in situations where employees are required by law to report criminal wrongdoings.

On the corporate governance side of the problem, there are a few reassuring indications that the landscape may be changing for the better. In our survey, for example, 35% of respondents from the region reported that their firms intend to invest in new or additional whistleblowing programs and anti-fraud staff training in the next 12 months. Although small relative to the proportion of businesses affected by employee-committed fraud, this figure is still above the global average of 28%.

Such spending is consistent with the growing recognition we find among our Gulf clients that internal reporting will have a direct impact on the reduction of fraud. That said, the success of a whistleblower program depends on several factors. Measures, such as an email address dedicated to internal audit, a fax machine in the corner of an office or the inclusion of superficial language in the company's code of conduct, singly or collectively, are inadequate and hardly constitute a whistleblowing program. In one case, Kroll found that an employee of a company did not report gross misconduct committed by the CEO because the Chief Compliance Officer responsible for dealing with whistleblower complaints who directly reported to the CEO. Such a scenario does not provide would-be whistleblowers with any confidence in how they might be treated if they report wrongdoing. And if wrongdoing is not being reported, the assumption is that a large percentage of fraud may well be undiscovered. With 42% of fraud committed by senior executives, it is important to maintain reporting lines to officers who are independent of, and isolated from, senior management.

We are often asked by clients how to establish an effective whistleblower program. There is no off-the-shelf solution, but rather the program must reflect the true nature of the company – its size, operations, geographies, activities, types of transactions, exposure and so on. Several key pillars, though, are universally necessary to facilitate the creation of an effective program. Firstly, and most importantly, corporate leadership must consciously and proactively create an overarching culture of disclosure and good governance and then support its implementation. This should lead to a number of other crucial elements of fraud control: robust internal audit and compliance functions; clear and obligatory contractual responsibilities for employees along with well-publicized rules and procedures; actionable code of conduct guidelines; transparency in how the fraud prevention system works; fraud response plans and; continual staff training. Embedded in this context, a specific whistleblower program requires well-publicized rules and procedures; independent hotlines; and clear policies on the management of information, including the treatment of those who provide it.

As for the second general problem noted above, the legal status and treatment of whistleblowers in civil and criminal matters are usually defined by labor laws and penal codes. To date, however, no country in the Gulf has overarching legislation that provides clarity (or comfort) regarding the treatment and status of whistleblowers or even the management and application of the information provided by them. However, a number of governments in the Gulf region are at the beginning of paving the way for appropriate legislation and procedures to be implemented. The United Arab Emirates, for example, is expected to establish a Federal Authority for Combatting Corruption (although the law has been drafted, at the time of publishing the Authority is yet to be established). The legislation will cover all types of wrongdoing in the private sector, including conflicts of interest, money laundering, breaches of trust, bribery and embezzlement. Relevant here, the legislation will also issue regulations regarding the protection of whistleblowers from civil, administrative or criminal prosecution. The Dubai Financial Services Authority, the regulator in the Dubai Financial International Center (an economic free zone that constitutes the financial district of Dubai), requires entities to have appropriate procedures and protections in place to facilitate the reporting of wrongdoing by employees. Although it does not extend to non-regulated entities or companies outside the free zone, the interplay between offshore and onshore businesses encourages a wider culture of compliance and reporting.

A complete discussion of whistleblowing in the Gulf requires two caveats. First, the region is not alone in providing insufficient whistleblower protection. Even in some developed economies around the world, the nature of those safeguards remains weak or is still evolving. In the Gulf, a region where financial markets were created only in the last two decades or so, it is understandable that gaps and challenges will exist for some time to come.

Secondly, improved whistleblowing programs are not standalone solutions to fraud. The information they provide may be incorrect or malicious in nature. One example from a recent case involved an email from a whistleblower that disclosed what appeared to be serious allegations of wrongdoing; when investigated, however, it transpired that the writer's motivation was to undermine a transaction involving the acquisition of a company. In less serious instances, some people inevitably engage in supposed whistleblowing because they feel aggrieved at being passed over for a promotion or pay raise, or wish to undermine a colleague or manager.

A properly designed and executed internal investigation will help senior executives consider the information provided by whistleblowers and decide on next steps. Their investigation needs to assess the severity of the situation and ensure that company systems and assets are not vulnerable to further attacks. A further key question is whether to call in external counsel or even the authorities—a decision largely driven by a company's industry and regulatory requirements.

It may be tempting to look the other way. We have encountered many situations where confusion and panic after a fraud has taken place have prevented corporates from implementing plans to combat internal fraud. Clients often fall victim to internal impediments and bureaucracy too, or even lack of budgets to deal with fraud. What might appear to be a small problem, though, is usually the tip of the iceberg. Failing to act on a tip-off can mean the company ends up spending more money after a regulator or public prosecutor becomes involved because in such cases these public officials take over and dictate the direction of the investigation.

The bottom line is that whistleblower programs are an essential tool in the perpetual struggle against crime, and one which companies – and governments – in the Gulf need to protect and employ better, especially if they are to bring down the region's high levels of fraud.

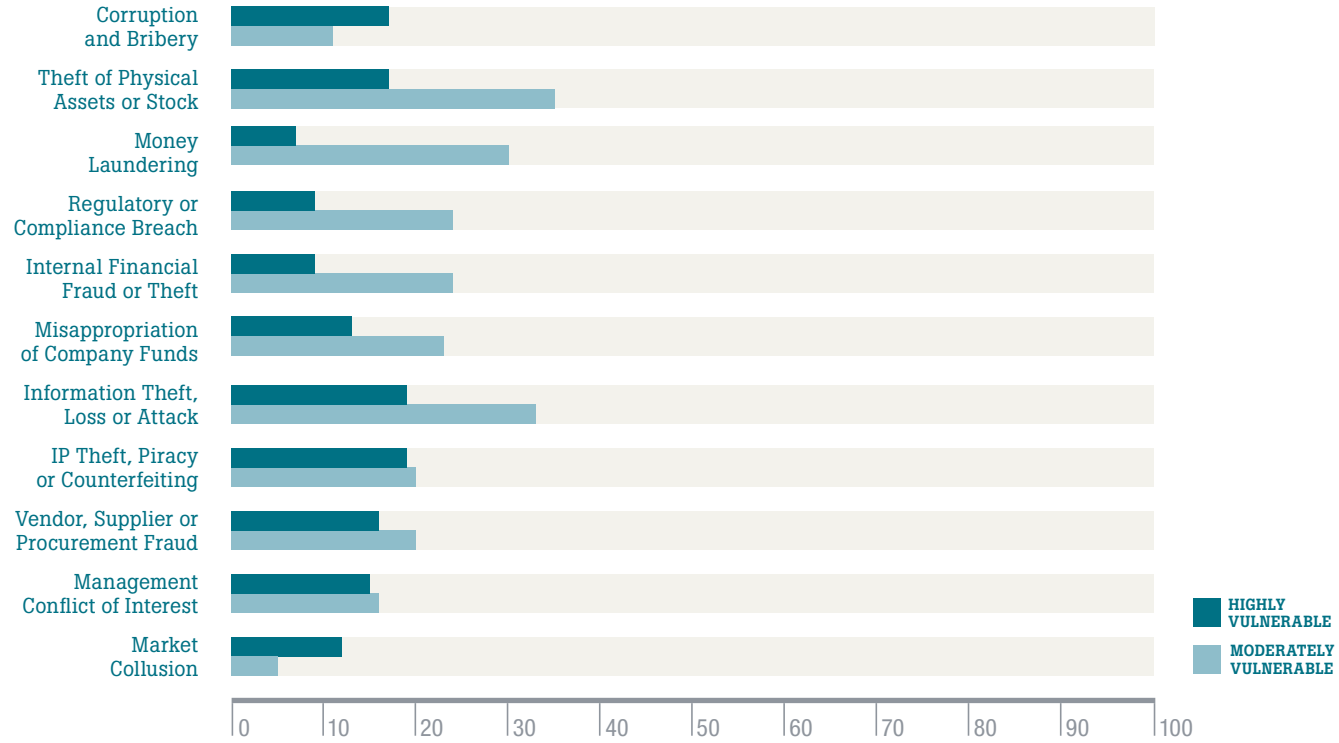
Yaser Dajani is Managing Director in Kroll's Dubai Office and Head of the Middle East. He manages investigations for regional and international businesses and government clients, and oversees a team of forensic investigators and business intelligence specialists in the Dubai Office. Yaser's core areas of expertise include complex business intelligence, internal investigations, dispute advisory, litigation support and asset tracing, anti-counterfeit support and corruption risk assessments.

ECONOMIST INTELLIGENCE UNIT REPORT CARDS

Written by

The Economist Intelligence Unit

TECHNOLOGY, MEDIA AND TELECOMS



The dominant feature of fraud in the technology, media and telecoms industry in the last year was an outsized problem in the area of information theft. Other results are often positive relative to the rest of the survey: the sector, for example, had the lowest levels of any for regulatory and compliance breach (7%) and of vendor fraud (7%). Counterbalancing that, though, and putting overall fraud prevalence (79%) at an above-average level is the 32% of sector firms experiencing information theft—nearly twice the proportion of the next highest in the survey, financial services (18%).

A substantial driver of fraud for firms in the sector have been employees. For those that have suffered an information theft or attack and know the culprit, 36% of the time employee malfeasance was involved. More broadly, for companies which suffered any kind of fraud in the last year and where the perpetrator had been discovered, 56% of executives report junior employees played a leading role—just below the survey high. Meanwhile, high staff turnover is exacerbating employee-related fraud risk at 41% of all firms.

The industry's level of concern and response, however, seem oddly muted. Only 52% of technology, media and telecoms executives say their firms are moderately or highly vulnerable to information theft, just above the survey average of 51%. Investment in IT security software and training of all employees is more widespread than average, yet in both cases the sector is not the leader despite its substantially bigger problem than most. As for employee-induced risk, industry respondents are less likely than those in the overall survey to say that their companies intend to strengthen background screening (33% to 37%).

It would be wrong to say that this sector has an above-average fraud problem overall, but it should pay more attention to employees and information theft, with the latter in particular a predictable challenge for a knowledge industry.

PREVALENCE: Companies affected by fraud

79%

LOSS: Average percentage of revenue lost to fraud

0.7%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Information theft, loss or attack **(32%)**
- Management conflict of interest **(15%)**
- Theft of physical assets or stock **(15%)**

INCREASE IN EXPOSURE

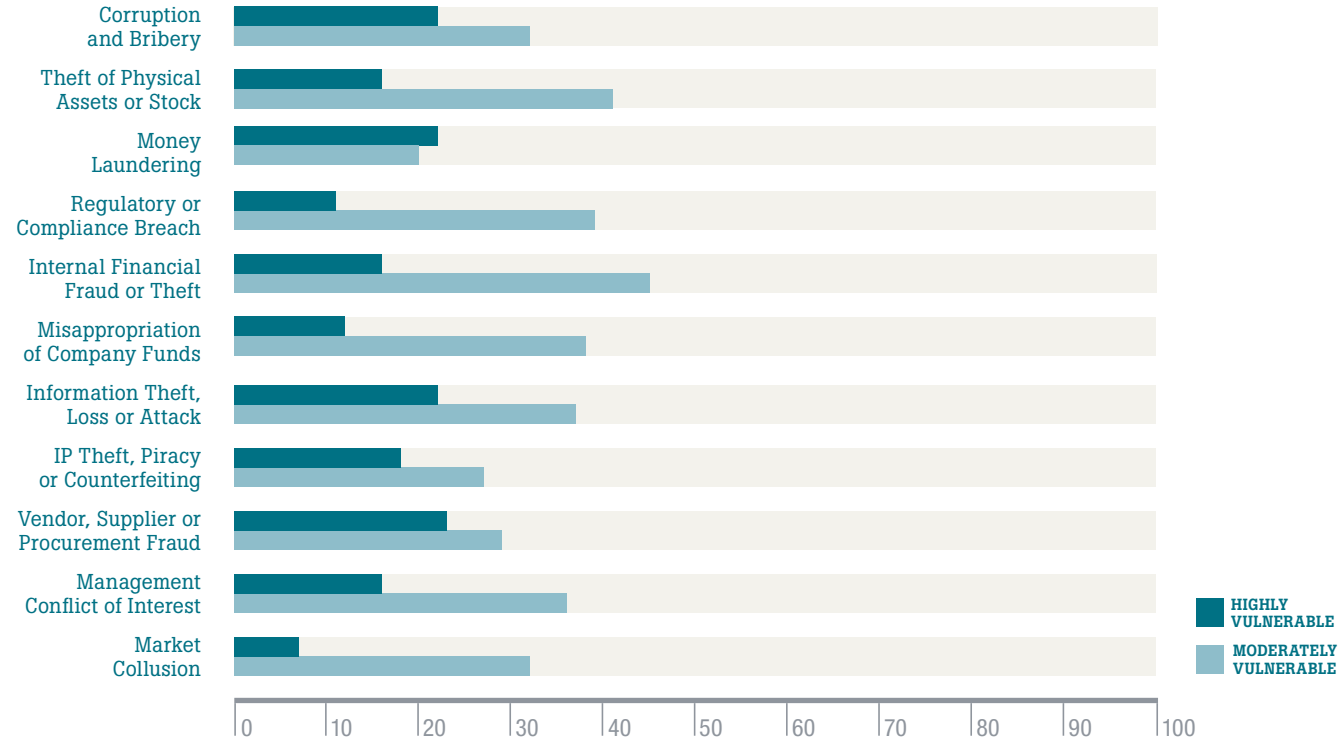
Companies where exposure to fraud has increased: **79%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(41%)**
- Increased outsourcing and offshoring **(15%)**

PROFESSIONAL SERVICES



The professional services sector presents a mixed fraud picture. On the positive side, its average loss to fraud (0.6% of revenue) is below that of the survey as a whole and the overall prevalence (72%) is less than average.

On the other hand, several weaknesses stand out. Over the last 12 months, the sector has had the highest incidence in any industry of corruption and bribery (22%) and of internal financial fraud (14%). It also had the second highest rate of money laundering (9%). The concerns of industry respondents suggest no rapid change. Professional services firms are the second most likely to report that they are moderately or highly vulnerable to corruption (54%) and to money laundering (42%), and the most likely to say this of internal financial fraud (61%).

As in past years, the data suggest that the sector's anti-fraud efforts need to address possible senior and middle management misbehavior. Professional services firms have above-average levels of management conflict of interest (13%) and over half of firms (52%) report themselves moderately or highly vulnerable to that fraud—again the highest in the survey. Similarly, the sector is unusual in being one of only two where senior and middle management are more likely than junior employees to be perpetrators of fraud. As outlined in the last report, partners need watching too.

PREVALENCE: Companies affected by fraud

72%

LOSS: Average percentage of revenue lost to fraud

0.6%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Corruption and bribery **(22%)**
- Internal financial fraud **(14%)**
- Information theft, loss or attack **(13%)**
- Management conflict of interest **(13%)**

INCREASE IN EXPOSURE

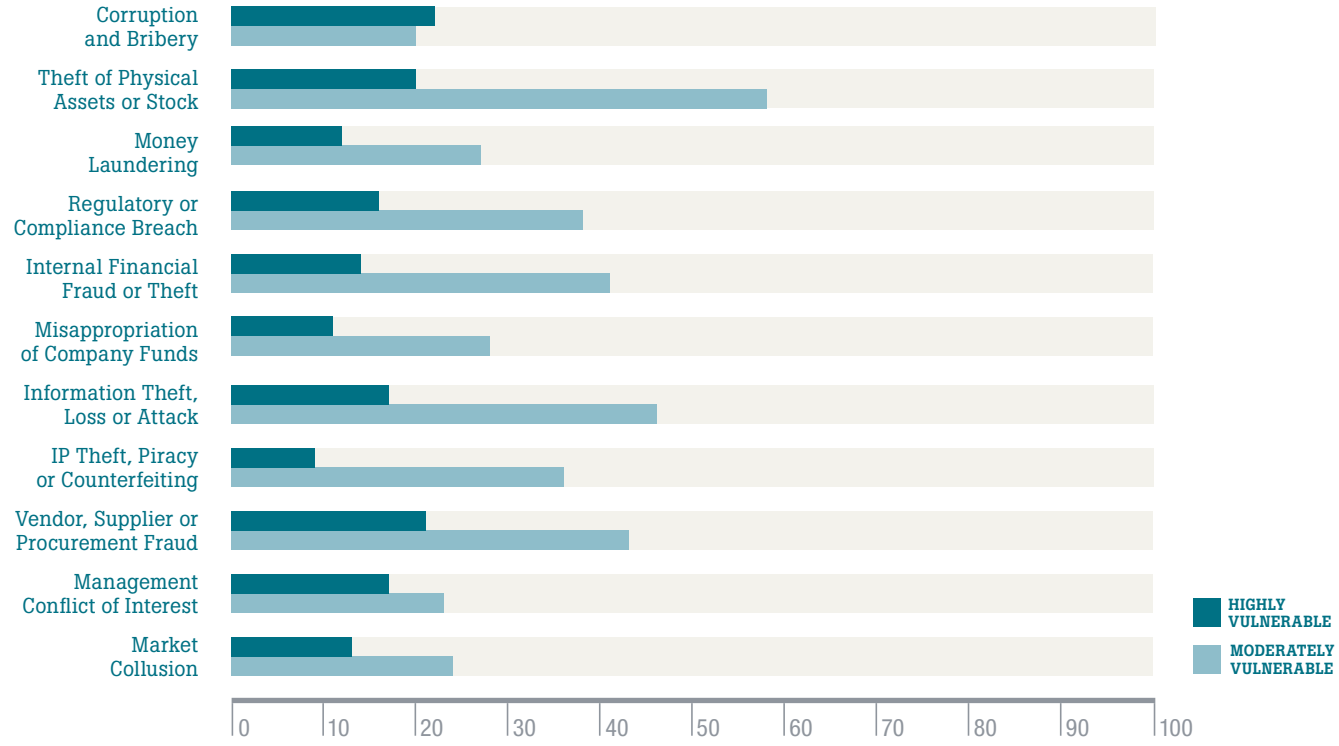
Companies where exposure to fraud has increased: **81%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(20%)**
- Increased outsourcing and offshoring **(19%)**

MANUFACTURING



Manufacturing had the most widespread fraud problem of any sector, with 82% being affected at least once. Not surprisingly, the sector also had the highest average loss to fraud at 1.1% of revenue. Looking at specific areas of weakness, it had the third highest rate of theft of physical assets (34%) and of vendor or procurement fraud (23%).

Consistent with the elevated level of vendor fraud, in the last year business partners and suppliers from outside the company posed a particular issue for the industry. At a third of all manufacturers which experienced fraud and where the perpetrator was known, a vendor or supplier was involved. Nearly one out of five times (18%) it was a joint venture partner. In both cases this is the highest figure for any sector, and manufacturing is the only industry this year where vendors were more often at fault than senior or middle management. Little wonder that increased collaboration between firms is one of the top drivers of increasing risk exposure, cited by 20%, once more the highest number for any industry.

The problem remains: manufacturers, for example, are the most likely to report that they are at least moderately exposed to vendor and procurement fraud (63%). On the other hand the industry seems to be taking steps in the right direction. Forty-three percent plan to invest in partner and supplier due diligence in the next year, substantially above the survey average of 33%.

PREVALENCE: Companies affected by fraud

82%

LOSS: Average percentage of revenue lost to fraud

1.1%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Theft of physical assets or stock **(34%)**
- Vendor, supplier or procurement fraud **(23%)**
- Information theft, loss or attack **(16%)**

INCREASE IN EXPOSURE

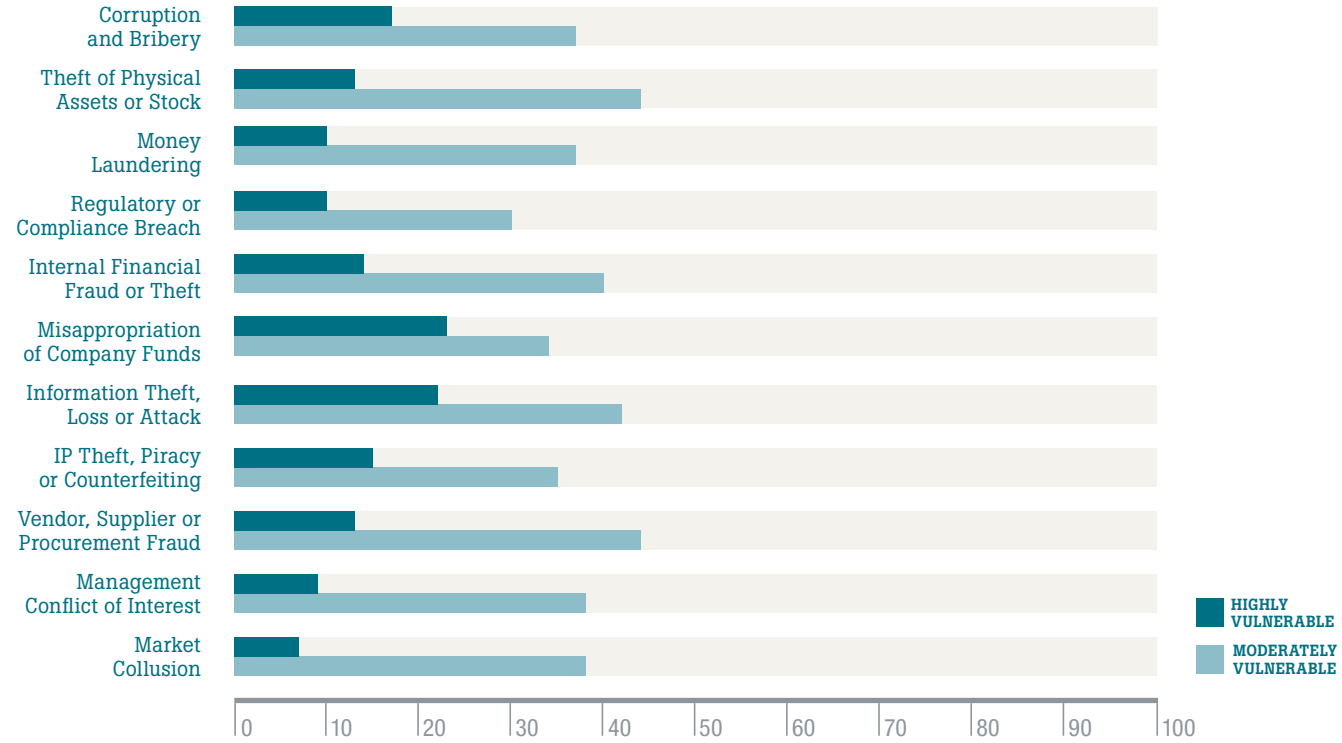
Companies where exposure to fraud has increased: **80%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(21%)**
- Increased collaboration between firms (joint ventures, partnerships) **(20%)**

NATURAL RESOURCES



The breadth of fraud in the natural resources industry poses a substantial challenge. In addition to above-average levels of vendor or procurement fraud (23%), the industry has the second highest incidence of regulatory or compliance breach (17%) and of corruption (16%). The latter two help explain why the industry was in the last year by some margin the one most likely to be taken advantage of by criminal government officials, which occurred at 14% of firms which experienced a fraud and where the culprit was known.

Although less extensive than the above crimes, the proportion of respondents from natural resources firms reporting misappropriation of funds (13%), money laundering (9%) and market collusion (4%) is the highest for any industry and, in each case, roughly double the average.

Given the variety of ways that fraudsters are attacking, it comes as no surprise that natural resources executives are the most likely to believe that their firms are moderately or highly vulnerable to six of the 11 frauds covered in the survey: information theft (64%), misappropriation of company funds (57%), corruption (55%), IP theft (50%), money laundering (47%) and market collusion (45%).

The industry is seeking to protect itself, with an above-average proportion investing in every anti-fraud measure covered in the survey except IT security, which nevertheless 59% of natural resources companies will still be spending money on. That said, the wide range of weak points will make such efforts an uphill battle.

PREVALENCE: Companies affected by fraud

77%

LOSS: Average percentage of revenue lost to fraud

1.0%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Vendor, supplier or procurement fraud **(23%)**
- Information theft, loss or attack **(17%)**
- Regulatory or compliance breach **(17%)**

INCREASE IN EXPOSURE

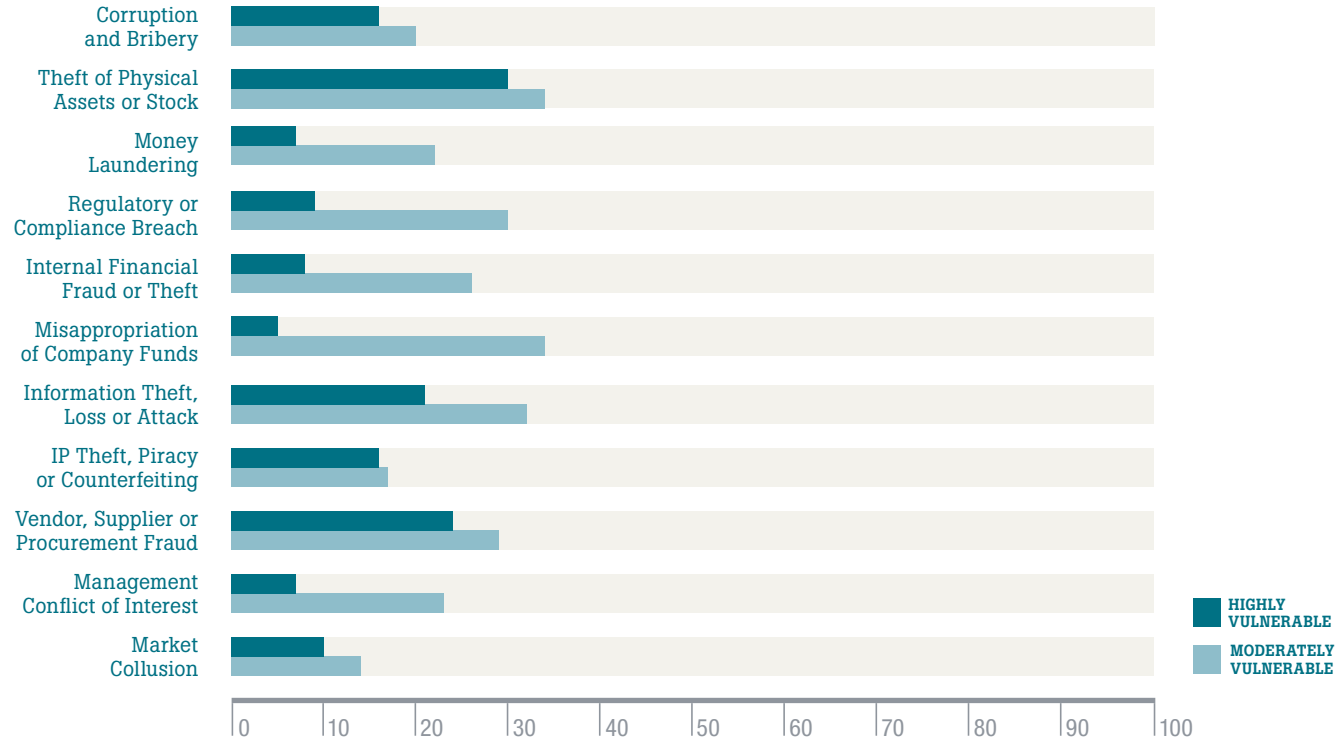
Companies where exposure to fraud has increased: **69%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(15%)**
- Increased collaboration between firms (joint ventures, partnerships) **(12%)**

CONSTRUCTION, ENGINEERING AND INFRASTRUCTURE



Construction has a number of large, and potentially growing, fraud issues. On the positive side, its average loss this year to fraud (0.6% of revenue) beat the survey average and the overall prevalence of fraud (75%) was the same as the all-industry mean.

Looking closer, the picture becomes more worrying. The sector had the highest rate of regulatory or compliance breach of any in the survey (18%), as well as the second highest figures for theft of physical assets (36%) and vendor or procurement fraud (24%).

The perpetrators are as big a challenge as the frauds themselves. Of those firms which suffered a fraud and where the perpetrator was known, in 42% of cases senior managers or middle managers played a leading role—tied for the highest figure in the survey—and in 51% of cases junior employees took an important part. Put another way, at just under a third (32%) of all construction firms in the last year, a senior executive or middle manager was found out taking part in a fraud against the company. On the other hand, insiders are also proving to be the best defense for these firms. At 30% of companies where a fraud was discovered, it was through the efforts of company management and in 51% of cases via a whistleblower, the highest and second highest figures in the survey, respectively.

Surprisingly, those surveyed indicate that the sector's responses to its problems are less extensive than those of peers in other industries. They are less likely to plan to invest in the coming year in management controls (25%) or background screening (30%) than the survey average (39% and 37%), respectively, and far less likely to be beefing up staff training and whistleblower hotlines to support their employees (17% compared with 28% overall). This may reflect an under-appreciation of the risk. Despite the elevated incidence of compliance breach, physical asset theft and procurement fraud, the proportion of construction executives believing that their firms are moderately or highly vulnerable is close to average.

With the highest increase in fraud exposure of any sector (92%), it might be wise for the industry to pay more attention to its defenses.

PREVALENCE: Companies affected by fraud

75%

LOSS: Average percentage of revenue lost to fraud

0.6%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Theft of physical assets or stock **(36%)**
- Vendor, supplier or procurement fraud **(24%)**
- Regulatory or compliance breach **(18%)**

INCREASE IN EXPOSURE

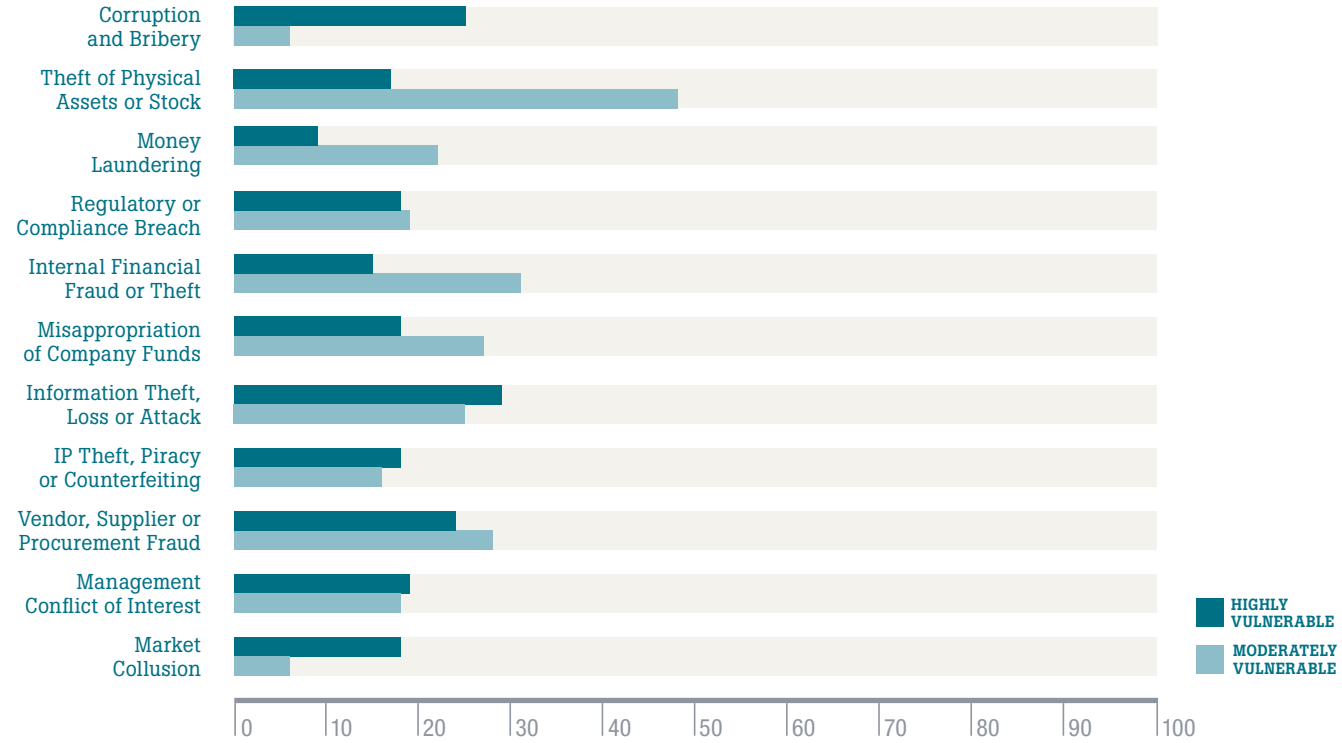
Companies where exposure to fraud has increased: **92%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(49%)**
- Entry into new, riskier markets **(21%)**

CONSUMER GOODS



The consumer goods industry's fraud experience last year was better than that of most others, but substantial concern exists among a minority of executives that vulnerabilities are greater than recent incidence would suggest.

Overall, the sector had a slightly below-average fraud prevalence (72% compared to 75% for the survey as a whole) and a comfortably below-average financial loss (0.6% of revenues compared to 0.8%). Similarly, for nine of the 11 frauds covered in the survey, the incidence was lower than the overall average, while for the two exceptions, vendor or procurement fraud (19%) and management conflict of interest (13%), it was only 2% and 1% higher, respectively.

Various data, however, point to a very concerned minority. For five of the 11 frauds covered in the survey, consumer goods respondents are the most likely to say they are highly vulnerable: information theft, loss or attack (28%); corruption and bribery (25%); management conflict of interest (19%); market collusion (18%); and regulatory or compliance breach (18%). More generally, 29% of consumer goods executives report that their businesses are highly vulnerable to three or more frauds, compared to just 21% for the survey as a whole. With such levels of concern, only time will tell whether this year's results were good fortune or the result of effective anti-fraud measures.

PREVALENCE: Companies affected by fraud

72%

LOSS: Average percentage of revenue lost to fraud

0.6%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Theft of physical assets or stock **(22%)**
- Vendor, supplier or procurement fraud **(19%)**
- Management conflict of interest **(13%)**

INCREASE IN EXPOSURE

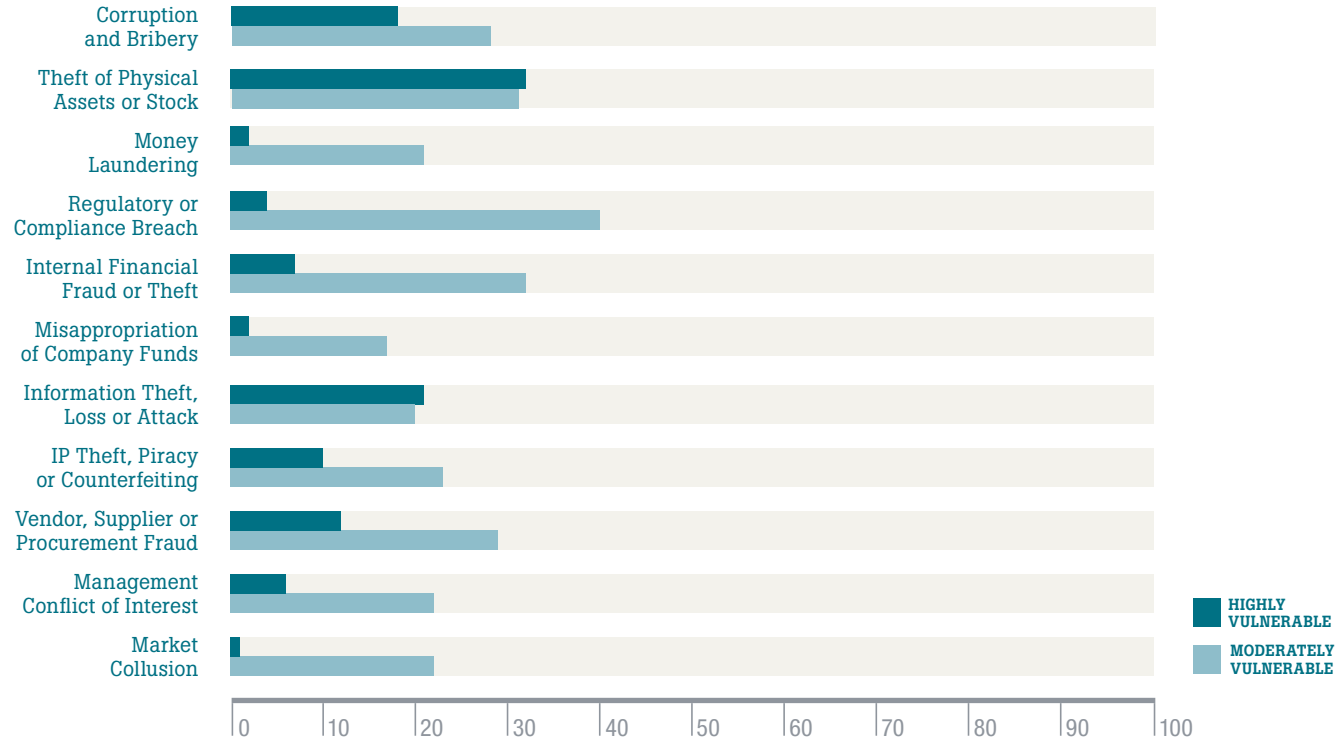
Companies where exposure to fraud has increased: **82%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(38%)**
- Increased outsourcing and offshoring **(18%)**

FINANCIAL SERVICES



An overall good year in keeping fraud down may be making the financial services industry more complacent than others about certain key issues.

Unusually, financial services companies has the second lowest prevalence of fraud in the survey, with only 70% of companies reporting being affected, and the lowest average loss (0.5% of revenues). The data also, however, point to a number of weaknesses. The sector saw the third highest proportion of firms affected by regulatory or compliance breaches (17%), the second highest for information loss (18%), and the highest for management conflict of interest (17%).

The last of these points to another pervasive attribute of financial services fraud: insider involvement. Among companies where fraud was uncovered in the past year and where the perpetrator is known, 42% report that senior or middle management took a leading role in at least one such crime, and a striking 58% say the same of junior employees. In both cases, this is the highest in the survey. The latter figure is the highest in the survey and the former tied for first place.

Looking ahead does not bring much comfort. The greatest driver of increased fraud exposure is high staff turnover which affects the businesses of 49% of financial services respondents—again tied for the highest level in the survey. Nevertheless, the industry is less likely than the survey average to plan to invest in the next year in either staff screening (31% compared to 37%) or management controls (28% to 39%). In fact, financial services respondents are less likely than average even to believe that they are moderately or highly vulnerable to management conflict of interest (28% versus 36%) despite the elevated incidence this year.

PREVALENCE: Companies affected by fraud

70%

LOSS: Average percentage of revenue lost to fraud

0.5%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Information theft, loss or attack **(18%)**
- Theft of physical assets or stock **(18%)**
- Management conflict of interest **(17%)**
- Regulatory or compliance breach **(17%)**

INCREASE IN EXPOSURE

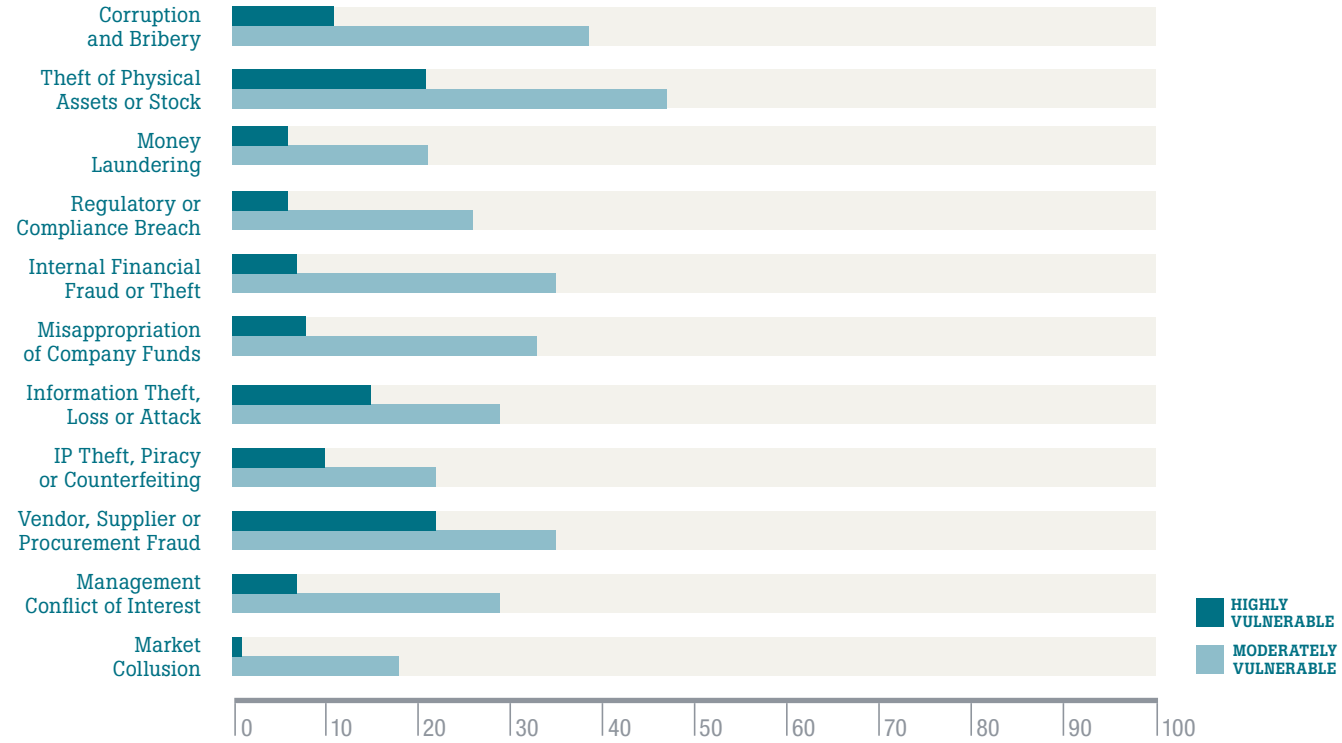
Companies where exposure to fraud has increased: **82%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(49%)**
- Entry into new, riskier markets **(20%)**

RETAIL, WHOLESALE AND DISTRIBUTION



Retail, wholesale and distribution had the second highest losses to fraud of any sector in the last year (1.1% of revenue). Its Achilles heel, as in the past, is theft of physical assets, reported at 46% of firms in the industry, the highest sectoral figure of any in the survey and more than twice the overall average (22%). Making matters worse, the industry also had the highest reported rate of vendor, supplier and procurement fraud (27%).

More often than in most other industries, junior employees are driving these high fraud figures. At over half of companies in the sector that have experienced a fraud and where the culprits are known, junior employees played a leading role (53%), comfortably above the average (44%). More striking, when that crime in question was information theft, loss or attack, in 71% of cases employee malfeasance was involved—higher than for any other sector.

It is therefore no surprise that high staff turnover is increasing the risk of fraud at 33% of companies in the industry. Only 34% of retail, wholesale and distribution companies, however, are looking to put money in background screening in the coming year—slightly less than the survey average. With the industry's current issues, plenty of work remains to be done.

PREVALENCE: Companies affected by fraud

79%

LOSS: Average percentage of revenue lost to fraud

1.1%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Theft of physical assets or stock **(46%)**
- Vendor, supplier or procurement fraud **(27%)**
- Information theft, loss or attack **(12%)**

INCREASE IN EXPOSURE

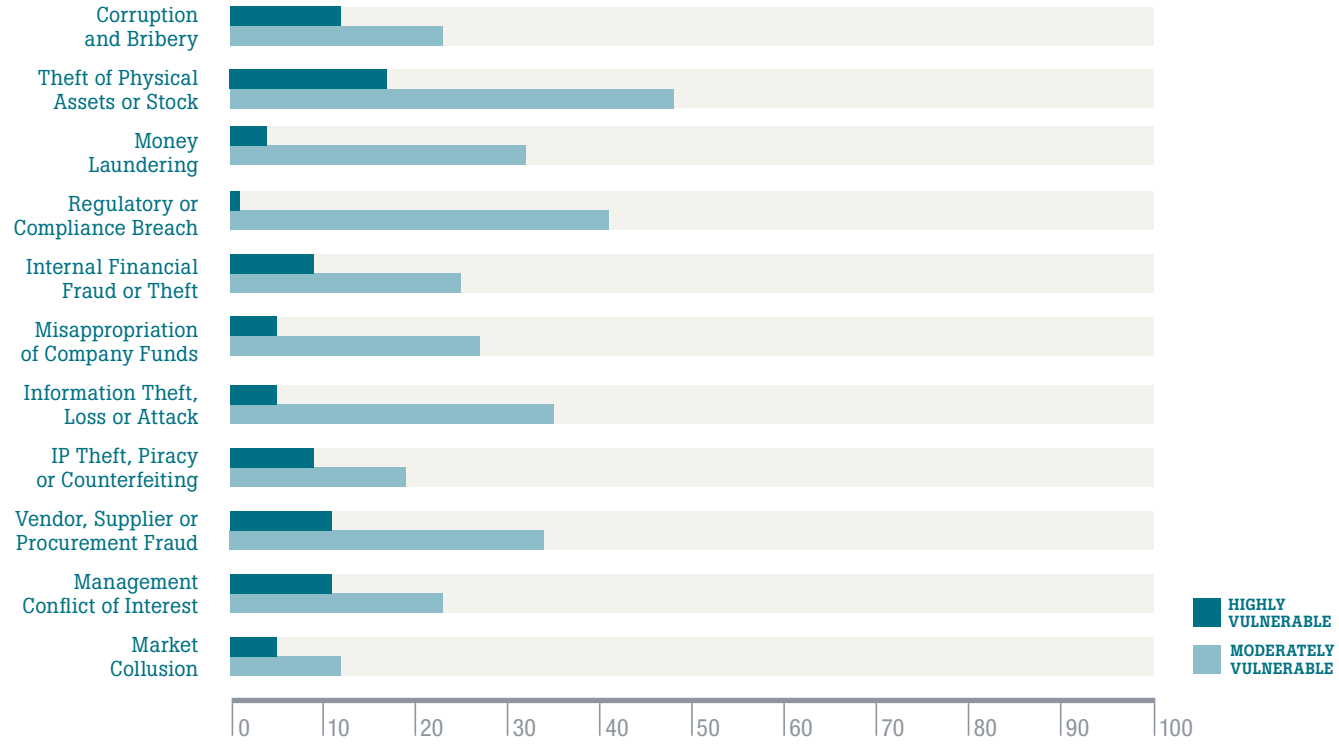
Companies where exposure to fraud has increased: **78%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(33%)**
- Entry to new, riskier markets **(16%)**

TRANSPORTATION, LEISURE AND TOURISM



The transportation, leisure and tourism industry has a very average fraud problem, but is acting as though it has a smaller one. The number of companies affected by at least one fraud (75%) is the same as for the survey as a whole and the average loss (0.9% of revenues) just slightly higher than the norm (0.8%). Looking at particular types of fraud, again little stands out from the average except that last year the sector reported the smallest incidence of regulatory or compliance breach (with 7% of firms affected) but the third highest rate of corruption (15%). Vendor and procurement fraud (20%) is also above average (17%).

What sets apart the sector from the norm is that it is less likely to be planning to enhance efforts to fight fraud in the year ahead. For nine of the 10 anti-fraud strategies covered by the survey, transportation, leisure and tourism executives are less likely than peers in other sectors to report intended investment. The sole exception is general risk management, and here the figure (31% plan to invest) is only slightly above the average (30%). Although the industry does not have unusual fraud problems, this should not be cause for complacency.

PREVALENCE: Companies affected by fraud

75%

LOSS: Average percentage of revenue lost to fraud

0.9%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Vendor, supplier or procurement fraud **(20%)**
- Theft of physical assets or stock **(15%)**
- Corruption and bribery **(15%)**

INCREASE IN EXPOSURE

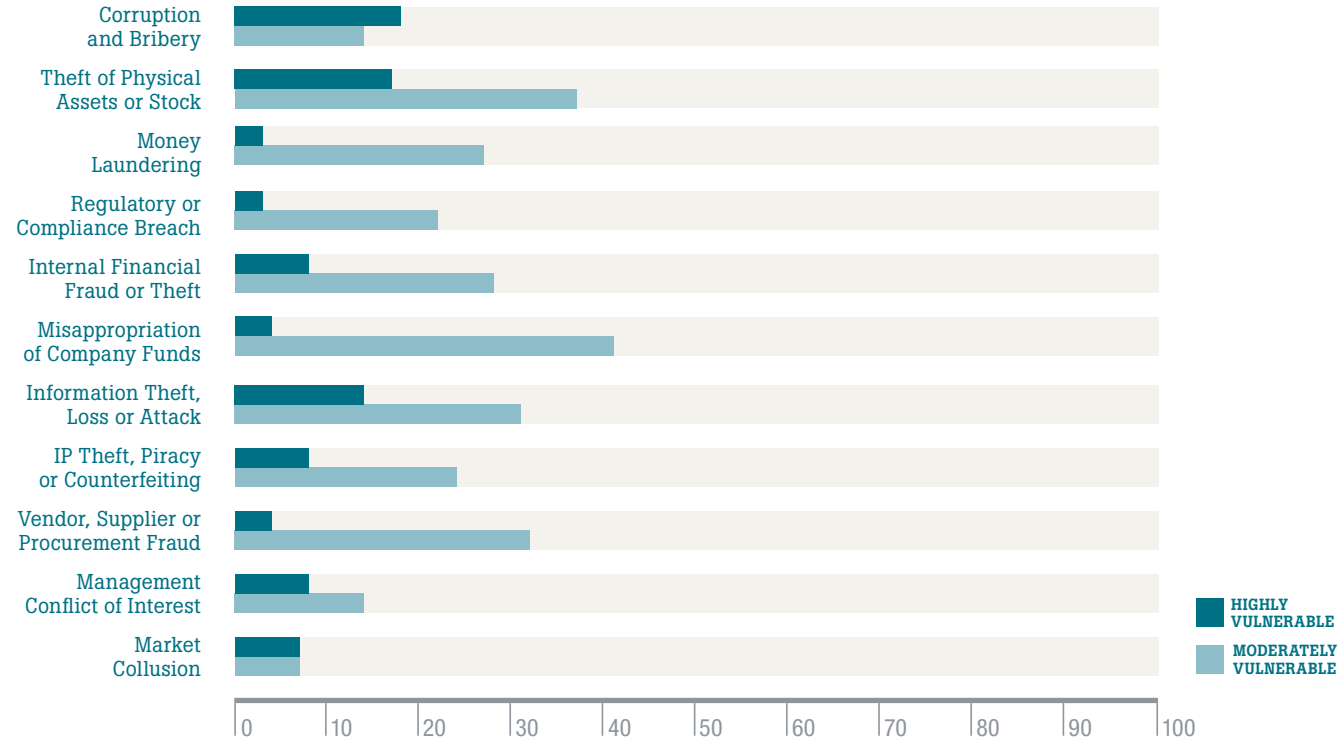
Companies where exposure to fraud has increased: **75%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(32%)**
- Entry into new, riskier markets **(15%)**
- Complexity of products and services sold **(15%)**

HEALTHCARE, PHARMACEUTICALS AND BIOTECHNOLOGY



The healthcare, pharmaceuticals and biotechnology industry had the lowest number of companies affected by fraud in the last year (69%), but that did not prevent it from having the most widespread problem with IP theft (13%), and the second biggest with management conflict of interest (17%). The frauds which sector companies experienced were also more expensive than average, as despite its very low incidence the mean financial loss to fraud (0.8% of revenues) was around the survey norm.

Healthcare companies, however, are not taking active measures to address the industry's weaknesses. Only 36% report that their firm will be investing in management controls in the coming year, below the survey average (39%). Moreover, and surprisingly for this industry, is the low focus on intellectual property measures. The proportion of respondents who say that their company will be enhancing IP protection in the coming year is 18%, but 19% report that increased outsourcing and offshoring—common routes for IP loss—have driven greater risk exposure. This latter is the highest figure for any sector in the survey. To keep fraud levels at those reported this year, the healthcare, pharmaceuticals and biotechnology industry will have to keep adapting its anti-fraud measures to its evolving business model.

PREVALENCE: Companies affected by fraud

69%

LOSS: Average percentage of revenue lost to fraud

0.8%

AREAS OF FREQUENT LOSS

Percentage of firms reporting loss to this type of fraud:

- Management conflict of interest **(17%)**
- Theft of physical assets or stock **(14%)**
- Regulatory or compliance breach **(14%)**

INCREASE IN EXPOSURE

Companies where exposure to fraud has increased: **78%**

BIGGEST DRIVERS OF INCREASED EXPOSURE

Most widespread factor leading to greater fraud exposure and percentage of firms affected:

- High staff turnover **(28%)**
- Increased outsourcing and offshoring **(19%)**

Contact Kroll

For information about any of Kroll's services, please contact a representative in one of our offices below or visit www.kroll.com

Corporate Headquarters

600 Third Avenue, New York, NY 10016

Global Representatives

North America
Bill Nugent
Philadelphia
1 215.568.8090
bnugent@kroll.com

Latin America
Recaredo Romero
Bogotá
57 1 742 5556
rromero@kroll.com

Europe, Middle East & Africa
Tom Everett-Heath
London
44 207 029 5067
teverettheath@kroll.com

Asia
Tadashi Kageyama
Hong Kong
852 2884 7788
tkageyama@kroll.com

Local Offices

North America

Dan Karson
New York
1 212.833.3266
dkarson@kroll.com

Pete Turecek
Boston
1 212.833.3373
pturecek@kroll.com

Jonathan Fairtlough
Los Angeles
1 213.443.1121
jfairtlough@kroll.com

Bill Nugent
Philadelphia
1 215.568.8090
bnugent@kroll.com

Betsy Blumenthal
San Francisco
1 415.743.4825
bblument@kroll.com

Jeff Cramer
Chicago
1 312.345.2755
jcramer@kroll.com

Peter McFarlane
Toronto
1 416.813.4401
pmcfarlane@kroll.com

Latin America

James Faulkner
Miami
1 305.789.7130
jfaulkner@kroll.com

Jorge Suescun Pozas
Bogotá
57 1 742 5556
jorge.suescunpozas@kroll.com

Brian Weihs
Mexico City
52 55 5279 7250
bweihs@kroll.com

Matías Nahón
Buenos Aires
54 11 4706.6000
mnahon@kroll.com

Snežana Gebauer
São Paulo
55 11 3897 0892
snezana.gebauer@kroll.com

Asia

Colum Bancroft
Hong Kong
852 2884 7788
cbancroft@kroll.com

Violet Ho
Beijing/Shanghai
86 10 5964 7600
vho@kroll.com

Reshmi Khurana
Mumbai
91 22 6724 0504
rkhurana@kroll.com

Richard Dailly
Singapore
65 6645 4521
rdailly@kroll.com

Omer Erginsoy
Singapore
65 6645 4530
oerginsoy@kroll.com

Naoko Murasaki
Tokyo
81 3 3509 7103
nmurasaki@kroll.com

Europe, Middle East & Africa

Zoë Newman
London
44 207 029 5154
znewman@kroll.com

Yaser Dajani
Dubai
971 4 449 6714
ydajani@kroll.com

Marcelo Correia
Madrid
34 91 274 7974
marcelo.correia@kroll.com

Marianna Vintiadis
Milan
39 02 8699 8088
mvintiadis@kroll.com

Alex Volcic
Moscow
7 495 969 2898
avolcic@kroll.com

Béchir Mana
Paris
33 1 42 67 81 46
bmana@kroll.com

kroll.com