Annual Edition 2011/12

Global Fraud Report

Economist Intelligence Unit Survey Results

Fraud concerns on the rise globally

Information theft remains a serious threat

Lack of preparation for greater regulatory enforcement

Businesses struggle with anti-fraud strategies

Kroll®

An Altegrity Company

About the research

The Annual Global Fraud Survey, commissioned by Kroll and carried out by the Economist Intelligence Unit, polled 1,265 senior executives worldwide from a broad range of industries and functions in June and July 2011. 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 and Wholesale; Technology, Media, and Telecommunications; Healthcare and Pharmaceuticals; Travel, Leisure, and Transportation; Consumer Goods; Construction, Engineering, and Infrastructure; Natural Resources and Manufacturing. Respondents were senior, with 47% at C-suite level. One-half of participants represent companies with annual revenues of over $500m. Respondents this year included 23% from North America, 24% from Europe, 28% from the Asia-Pacific region, 15% from the Middle East/Africa and 11% from Latin America.

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 US dollars.

Global Fraud Report Contents

Introduction

All businesses are confronted with the risk of fraud. How they respond – the nature of their approach to prevention, detection, investigation and disclosure – will separate those who manage through the issues from those who suffer significant loss.

Organizations operating in multiple geographies, legal environments and cultures face a complex set of challenges and risks as they develop their business. This fifth edition of Kroll's Global Fraud Report, prepared in cooperation with the Economist Intelligence Unit, illustrates the speed at which the fraud threat is evolving, and reinforces the direct financial benefit to those organizations who actively manage their fraud risk.

A positive finding in this years' report is a drop in the overall prevalence of fraud – from 88% of respondents having suffered an incident in the last 12 months to 75%. However, a number of specific fraud types are growing more common: in particular, management conflict of interest, supply chain fraud, internal financial fraud and corruption are of mounting concern. Companies must stay vigilant as today's fraudsters are increasingly sophisticated in the structuring of their crimes and the tactics deployed to prevent detection.

There are some points of particular note that emerge from this year's survey;

- **Awareness**. Awareness and concern about fraud has risen markedly – even as, or perhaps partly supporting, an overall decrease in the number of businesses suffering a fraud incident in the last 12 months.
- **Evolution**. The good news is that the two biggest areas of fraud – theft of physical assets and theft of information both saw small declines this year, but fraudsters are evolving and other fraud areas, especially those linked most closely to the firms' own employees and supply chain partners, have gone up sharply.
- **Corruption**. Half of our respondents were moderately or very concerned about corruption while the incidence of corruption doubled.
- **Preparedness**. Despite the rise in corruption concerns, companies are still unprepared for greater regulatory enforcement. Less than 30% of respondents believe their companies have trained their managers, vendors and foreign employees to be both familiar and compliant with the UK Bribery Act or US Foreign Corrupt Practices Act, and less than one quarter believe their pre-transactional due diligence identifies a target's compliance with the Acts.
- **Anti-Fraud measures pay**. Our survey suggests that any company can be the victim of fraud, but consistently and across industries and geographies, the biggest victims of fraud invested the least in the unglamorous disciplines of training, audits, screening and due diligence.

The Report presents the collective input of some of the world's most talented and diligent anti-fraud practitioners. I hope it provides some useful insights and helps you identify emerging threats and opportunities for your own business.

Tom Hartley
Global Head
Business Intelligence & Investigations

Economist Intelligence Unit Overview

This report, the fifth and biggest annual Economist Intelligence Unit Global Fraud Survey, commissioned by Kroll, polled more than 1,200 senior executives worldwide from a broad range of industries and functions in June and July 2011. As ever, it found fraud to be pervasive and protean, with progress made in some areas almost inevitably matched by increasing risks in others. The data this year provides four key insights about the current fraud environment.

1. Concern is rising about every type of fraud as businesses face a more varied threat.

On the surface, the 2011 survey contains some good news. The number of companies affected by the two most common types of fraud has declined. This year, 25% report experiencing theft of physical assets (down from 27% in the 2010 survey) and 23% suffered from information theft, loss, or attack (also down from 27%). More broadly, only 75% of companies were victims of a fraud in the last 12 months, a noticeable drop from last year's figure of 88%, and one of the lowest totals since the survey began.

Companies, however, are anything but relaxed: instead, the level of concern has increased sharply among respondents. For every fraud covered by the survey, the proportion of respondents saying that their business is highly or moderately vulnerable has risen, usually by between 10% and 15%. Even for theft of information and physical assets, which declined from 2010, concern has grown.

What can we make of this? It may take further years of survey data to demonstrate an absolutely clear trend, but this year's figures suggest the beginning of a broad shift in the fraud environment. Fraudsters may not be obviously seen to be engaging in theft of physical assets and information as they may have been previously, but that does not mean they are giving up. Instead, other frauds are becoming much more common, in particular internal financial fraud, corruption, and vendor or procurement fraud.

As a result, instead of an environment where there are two leading risks and a number of other smaller issues, companies now face a range of more widespread dangers. In particular, after the two most common frauds, the next four—management conflict of interest, procurement fraud, internal financial fraud, and corruption—hit roughly one in five companies last year, and financial mismanagement was close behind at one in six. This rapid shift in the nature of the fraud threat explains the increase in a sense of vulnerability. Fraudsters have been deploying a range of tools to probe corporate defenses rather than just relying on one or two, for the most part. Whether this shift continues, and how successful companies will be in tackling it, will become clear only in future surveys.

Chart I: Proportion of companies describing themselves as highly or moderately vulnerable to the following frauds

	2011	2010
Information theft	50%	38%
Corruption and bribery	47%	38%
Theft of physical assets	46%	34%
Management conflict of interest	44%	27%
Vendor, supplier or procurement fraud	42%	26%
Regulatory or compliance breach	41%	30%
IP theft	40%	27%
Financial mismanagement	39%	30%
Internal financial fraud	38%	27%
Market collusion	31%	N/A
Money laundering	25%	19%

Chart II: Percentage of companies affected by listed frauds

	2011	2010
Theft of physical assets	25%	27%
Information theft	23%	27%
Management conflict of interest	21%	19%
Vendor, supplier or procurement fraud	20%	15%
Internal financial fraud	19%	13%
Corruption and bribery	19%	10%
Financial mismanagement	16%	13%
Regulatory or compliance breach	11%	12%
IP theft	10%	10%
Market collusion	9%	7%
Money laundering	4%	7%

2. Companies are growing increasingly aware of their exposure to corruption but often still do not have structures in place to address it.

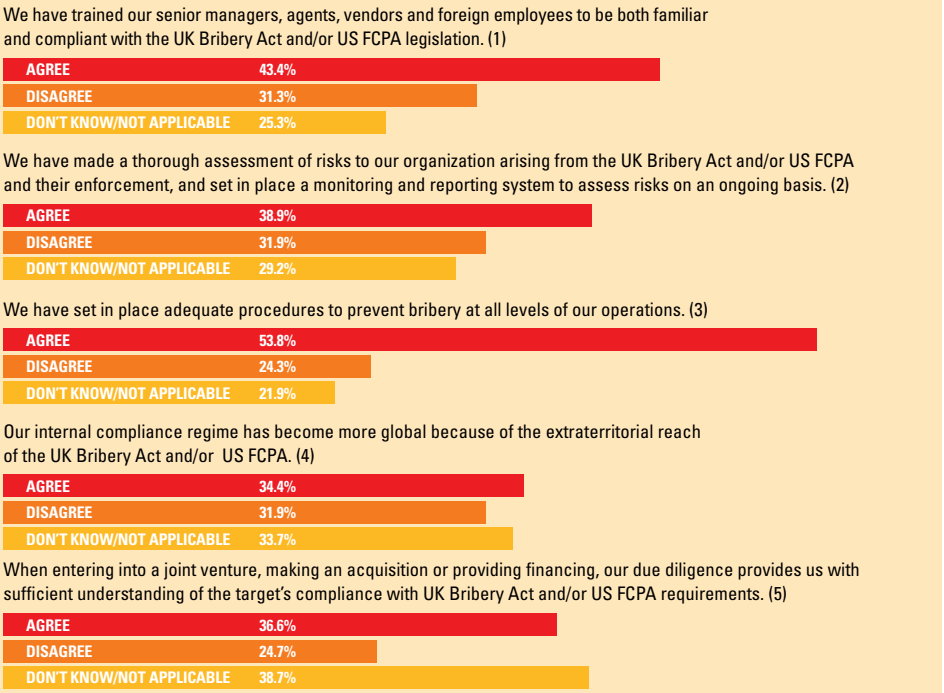
Corruption is a growing risk for companies worldwide. Its prevalence has shown the biggest increase of any of the frauds covered in the survey, nearly doubling from 10% last year to 19% in the latest survey. This is occurring in an environment of ever greater regulatory scrutiny. The United States authorities have for some years now been increasingly vigorous, and extraterritorial, in their enforcement of the Foreign Corrupt Practices Act (FCPA). Britain's Bribery Act, which entered into force this July and also applies extraterritorially, is in some ways even tougher than the American legislation. It applies to bribes of individuals rather than just government officials, imposes a corporate duty to prevent bribery, and forbids facilitation payments. These are only the most prominent examples of greater regulatory rigor. Other countries, including China and India, have been toughening their legislation, although the effects on the ground remain to be seen.

As a result, concern about corruption has grown to the extent that it is one of the biggest fraud issues for companies: 47% now describe themselves as at least moderately vulnerable to corruption, more than for every fraud except information theft. More strikingly, 24% say that they are highly vulnerable to corruption, more than triple the level last year and the highest figure for any fraud in the survey.

This is having an impact on investment decisions. As was the case last year, this year's survey indicates that when fraud dissuades companies from doing business in a country or region, corruption is by far the biggest specific concern: of the 46% of companies that were dissuaded from operating somewhere by one or more types of fraud, 62% cited the presence of corruption as one of the leading issues in this decision. In the three regions that saw the largest number of respondents dissuaded from operating—Africa (15%), China (10%), and India (9%)—corruption was cited as a leading cause for the decision 69%, 59%, and 65% of the time respectively.

Despite such high concern, however, companies seem ill-prepared to deal with the issue. One-quarter admit that they are not very well prepared or not at all prepared to comply with regulations in this field, and only 27% say that they are well prepared. A deeper look at the data surrounding compliance with the FCPA and Bribery Act suggests that the problem is even bigger. Although these laws have an extraterritorial effect that can even have implications for non-American and non-British companies if they have certain links to the United Kingdom or the United States, it is possible that a foreign company's activities do not fall under the scope of either. This analysis therefore looks only at those respondents based in one of the two countries, as it would be difficult to imagine scenarios where their companies were not subject to the provisions of at least one of these pieces of legislation. Of those respondents, only 43% have trained senior management, agents, vendors, and foreign employees to be compliant with one of these laws, and just 39% have assessed the risks arising from them. These figures are not that much higher than the number of companies which definitely have not done so. Often, respondents simply do not know if they have—which suggests at the very least that any efforts have not had a high profile.

Chart III: How companies are reacting to the UK Bribery Act and US FCPA (British and United States-based respondents only)



Nor have due diligence processes caught up with the problem. Only 37% of respondents say that their companies provide a sufficient understanding of a potential partner's or investment target's compliance with these acts. Errors here can get expensive. In 2007, eLandia, a networking technology company, bought Latin Node, a wholesale provider of Internet telephony. Upon discovering evidence of corrupt payments at its new subsidiary, eLandia did everything right (informing authorities, firing implicated executives, terminating contracts obtained illegally), but the costs of all these actions mounted up and took a toll on the subsidiary's operations. Within a year, eLandia decided that the best option was to wind up Latin Node completely, losing its entire $22m investment in the process.

It is good that companies are aware of the problem corruption represents. They now need to do something about it.

3. The battle against information theft remains a leading focus for companies.

The prevalence of information theft declined in the last year, from 27% to 23%, but that does not mean that companies are confident that they have the problem under control. Instead, their concerns have increased.

One-half of respondents consider themselves moderately or very vulnerable to this fraud, up from 38% in 2010. IT complexity is the leading cause of increasing fraud exposure in the survey, cited by 32% of respondents, up from 28% last year. It is therefore no surprise that IT security is the most widespread anti-fraud investment planned for the coming year (30%).

Part of the reason for this concern may be that, typically, information theft tends to be more expensive than the other most widespread fraud, physical theft. When looking at companies that suffered only information or physical theft—in order to assess the impact of each—we can see that those hit by information theft lost more money. On average, victims of physical theft and no other crime lost 1.5% of earnings to fraud, while those hit by information theft lost 1.9%, suggesting that the latter is substantially more expensive.

Moreover, the nature of the information being sought by fraudsters is also widespread, requiring potentially different defenses for distinct types of data. As the chart shows, proprietary data is the most frequent target, but customer and employee data are also common goals. The prevalence of these targets obviously varies between industries depending on the value of the information a company is likely to have. For technology, media, and telecoms companies, proprietary data is the most common target (cited by 36% of respondents), while for financial services it is customer information (29%).

Overall the ongoing investment in information security may have yielded some positive results this year, but this is a battle far from won.

4. Those hit hardest by fraud often have no one but themselves to blame.

This year's fraud survey calculates the economic cost of fraud in a new, more direct way by asking respondents what proportion of revenue their company has lost in the last year. Most companies lost something, and for the survey as a whole, fraud cost companies 2.1% of earnings in the last 12 months—looked at in a different way, this equates to a whole week's revenue over the course of a year—which varies only modestly by geography or company size.

Looking just at the overall average, however, hides a group of 18% of companies that lost more than 4% of revenues to fraud. Fifty-three businesses, or just under a quarter of this group, were particularly badly hit, losing more than 10% of their revenue to fraud. Analyzing these firms—here called the "most affected"—reveals certain common characteristics.

The first lesson is that anyone can be hurt. Geography and industry are certainly factors, but not dominant ones: African and Middle Eastern companies are slightly over-represented (19% are among the most-affected, higher than their weight in the survey overall of 15%); and the group had a greater proportion of financial services firms (28%) than would be expected from their prevalence in the overall survey (17%).

The bigger differences are in how these companies deal with the risk of fraud.

To begin with, their defenses are weaker. As the chart shows, they are much less likely to have invested in any of the anti-fraud measures covered in the survey.

These poorer defenses leave the most affected much more open to fraudsters, and respondents are aware of this fact. A higher proportion of those surveyed from these

Chart IV: If your company has suffered information loss, theft or attack, what kind of information was targeted

Personally identifying information – customers	16.7%
Personally identifying information – employees	11.9%
Personal health information	2.8%
Proprietary data, including intellectual property	20.6%
Other	6.5%
Don't know	8.3%
We haven't suffered from this kind of fraud	47.4%

Chart V: In which of the following anti-fraud measures does your company currently invest

	Survey Average	Over 10% of revenue lost to fraud
Financial (financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)	72%	60%
Information (IT security, technical countermeasures)	66%	42%
Assets (physical security systems, stock inventories, tagging, asset register)	62%	40%
Management (management controls, incentives, external supervision such as audit committee)	52%	38%
Employee background screening	47%	36%
Staff (training, whistleblower hotline)	44%	21%
Partners, clients and vendors (due diligence)	43%	30%
Reputation (media monitoring, compliance controls, legal review)	41%	21%
Risk (risk officer and risk management system)	42%	26%
IP (intellectual property risk assessment and trademark monitoring program)	34%	19%

Chart VI: Proportion describing themselves as highly vulnerable to the following frauds

	Survey Average	Over 10% of revenue lost to fraud
Corruption and bribery	24%	51%
Theft of physical assets	13%	24%
Management conflict of interest	13%	24%
Vendor, supplier or procurement fraud	13%	19%
IP theft	13%	17%
Information theft	13%	17%
Regulatory or compliance breach	11%	30%
Financial mismanagement	10%	27%
Market collusion	9%	24%
Internal financial fraud	9%	15%
Money laundering	8%	30%

companies reports being highly vulnerable to every fraud in the survey, with the differences particularly large for corruption, money laundering, and regulatory breach. Similarly, these companies are less likely to say that they are well or reasonably well prepared to cope with compliance requirements relating to corruption, data, anti-trust rules or financial regulation, or to have set effective anti-bribery safeguards in place throughout the company.

They may know that they have a problem, but that is not enough to galvanize these companies into action. They differ little from the survey average in terms of their intention to invest further in anti-fraud measures. Moreover, even existing anti-fraud controls are too often not being well-maintained. Among the most affected, the leading contributor to increased fraud exposure, cited by 36% of respondents, is weakening of internal controls. In the survey as a whole, only 22% reported this problem, as did just 8% of those who suffered no financial loss.

Such controls, however, are essential for lowering the incidence of fraud. Last year, the survey found that more often than not fraud is an inside job. This year, if anything, this is even more the case: for those companies that have experienced fraud and where the culprit is known, 28% report that the fraudster was a junior employee and a further 21% say it was a senior employee (both figures were 22% last year). For a further 11%, the crime was committed by an agent or intermediary, meaning that overall 60% of fraud this year was carried out by someone who worked for the company one way or another—up from 55% last year.

Not only do companies clearly need strong controls, those controls need to be properly implemented throughout the organization. Even though junior employees are most often the culprits, they are not the most expensive fraudsters. For the most affected, senior executives are to blame in 29% of cases and junior ones in only 8%, while for those losing less than 1% to fraud, the figures are 20% and 35%. The more senior the potential fraudsters, the more rigorous a company's controls need to be in order to prevent their schemes.

It is hardly surprising that those who do less to protect themselves from fraud are more likely to suffer the consequences, but the number of companies losing a substantial portion of revenue suggests that it is a point worth restating.

Fraud Fatigue

By Tommy Helsby

Our annual survey in this edition of our Fraud Report shows a small decline in fraud. Have we turned the corner? Is fraud beginning to decline? Are fraud prevention measures finally starting to make inroads into corporate crime?

The answer is probably "no." The survey is an effective barometer of senior executives' awareness of fraud as a corporate risk. It shows the trends in different regions and in various areas of fraud vulnerability. The numbers probably say more about what business people are thinking than about the real size of the problem. The financial crisis of 2008–9 put a focus on fraud that pushed it very high on the corporate agenda for the past two years. There are, though, plenty of pressing matters competing for executive attention and therefore a danger that fraud risk – generally an uncomfortable subject and an unquantifiable exposure – is becoming neglected. Bluntly put, people may be getting bored with fraud.

Before the pendulum swings back too far in the wrong direction, it's worth reviewing how we got here to learn some useful lessons. As Warren Buffett said, "You only learn who has been swimming naked when the tide goes out." When times are good and profits are high, a fraud might be treated as an "accounting correction"; but when things are tough, that correction may result in a breach of banking covenants. When businesses fail, there is a natural desire to hold someone responsible, even to accuse that person of fraud – often with some justification, although the suspect will probably claim desperately that it was just "market practice." Certain "market practice" may now be recognized as, at best, improper and, sometimes, illegal; and politicians are finding that what used to be "unnecessary red tape" has become "essential tightening of the regulations." Regulators are encouraged – and empowered – to take no prisoners and, in response, the corporate compliance department is transformed from a backwater to a core component of business strategy.

Of course, I have over-simplified, but I think most people would recognize the outline of the story and many would agree that the result was a good thing, long over-due. You can, however, have too much of a good thing: no one wants regulators turning into vigilantes, the compliance police patrolling company corridors, and executives seeking legal advice on whether to choose a latte or a cappuccino at Starbucks. And of course, the press, conference organizers, and even on occasions corporate advisors such as us are inclined to fan the flames. The result, not surprisingly, is fraud fatigue. There needs to be a balance and some simple principles are worth keeping in mind in order to achieve it.

The risk of fraud is real. The financial crisis did not make it worse; it simply made it more apparent and, perhaps, made the consequences more serious. Most of the frauds took place during the good times, when our guards were lowered. Fraud prevention is important and needs to be proportionate and relevant to fraud vulnerability. As that vulnerability evolves along with how business is conducted – from paper ledgers to computer files, from cash-in-transit to electronic fund transfer, from physical assets to intellectual property – so must prevention techniques develop. Spotting the financial crime trends helps to anticipate where efforts need to be focused.

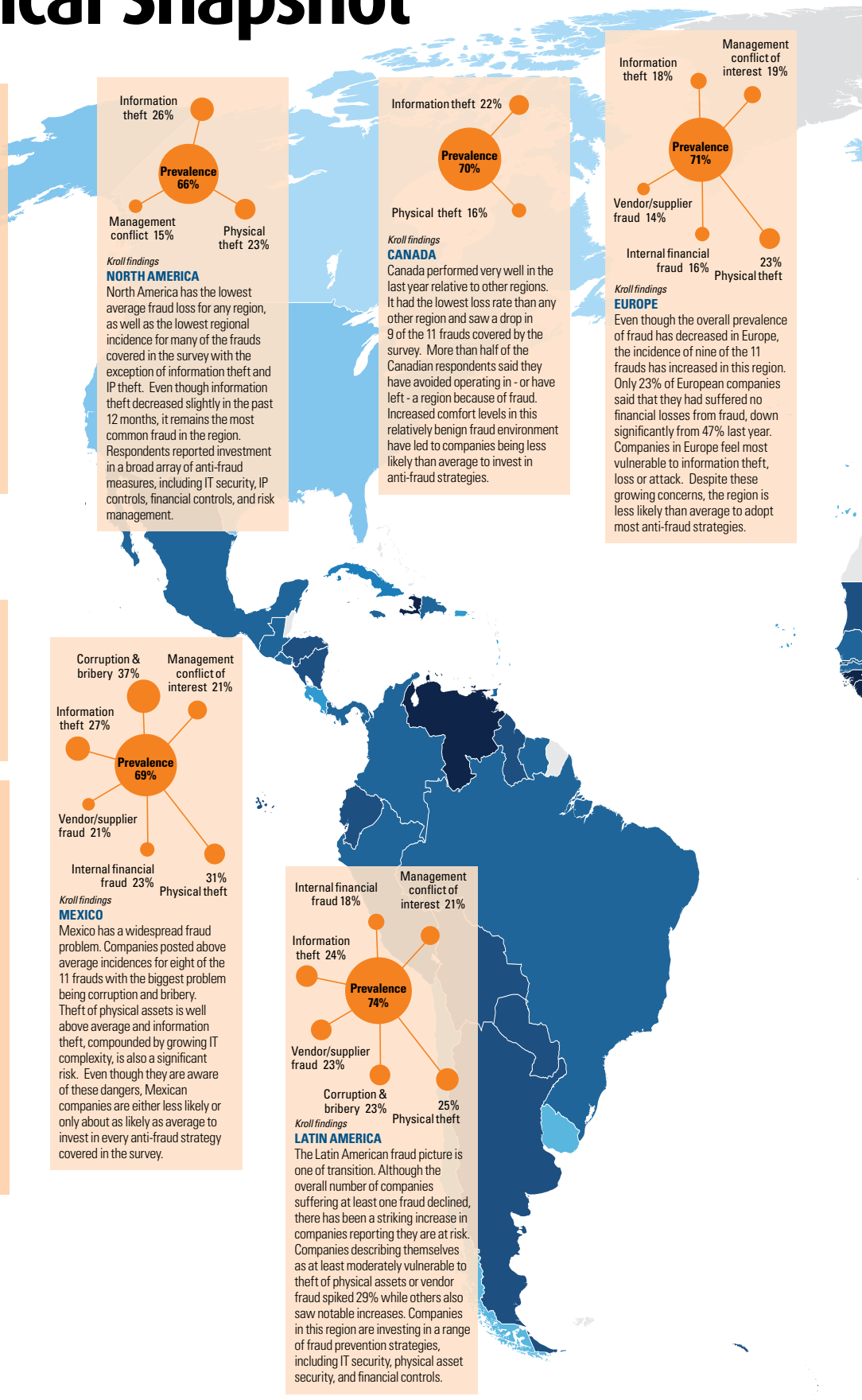
Compliance systems and controls are a key part of the defense against fraud, but compliance should not become an end in itself, perhaps not even a means to an end. We should aspire to be compliant not because the compliance departments tells us to but because that is the best way to run our businesses. Separation of duties in the accounts department picks up errors far more often than it does the occasional fraud. Contracts won through open competition are more valuable than ones awarded thanks to bribes. Background checks on vendors and agents will help weed out the incompetent and the inappropriate as well as the Minister's brother-in-law. The central mission of compliance needs to be maintaining and developing a well-founded and enduring business.

It is simple to say but may not be so easy to put into effect, particularly in an environment where transgressions are being treated more harshly. If we don't get it right, though, there is a real possibility that the pendulum will swing back to the laissez-faire past of rule-bending and blind eyes, of regulatory capture and arbitrage, and the cycle will start again.

Tommy Helsby is Chairman of Kroll Eurasia 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.

A Geographical Snapshot

We compared the results of the Global Fraud Survey findings with Transparency International's Corruption Perceptions Index (CPI). The CPI measures the perceived levels of public sector corruption as seen by business people and country analysts; ranging between 10 (very clean) and 0 (highly corrupt). The comparison clearly demonstrates that fraud and corruption frequently go hand in hand.



Kroll findings

NORTH AMERICA

North America has the lowest average fraud loss for any region, as well as the lowest regional incidence for many of the frauds covered in the survey with the exception of information theft and IP theft. Even though information theft decreased slightly in the past 12 months, it remains the most common fraud in the region. Respondents reported investment in a broad array of anti-fraud measures, including IT security, IP controls, financial controls, and risk management.

Kroll findings

CANADA

Canada performed very well in the last year relative to other regions. It had the lowest loss rate than any other region and saw a drop in 9 of the 11 frauds covered by the survey. More than half of the Canadian respondents said they have avoided operating in - or have left - a region because of fraud. Increased comfort levels in this relatively benign fraud environment have led to companies being less likely than average to invest in anti-fraud strategies.

Kroll findings

EUROPE

Even though the overall prevalence of fraud has decreased in Europe, the incidence of nine of the 11 frauds has increased in this region. Only 23% of European companies said that they had suffered no financial losses from fraud, down significantly from 47% last year. Companies in Europe feel most vulnerable to information theft, loss or attack. Despite these growing concerns, the region is less likely than average to adopt most anti-fraud strategies.

Kroll findings

MEXICO

Mexico has a widespread fraud problem. Companies posted above average incidences for eight of the 11 frauds with the biggest problem being corruption and bribery. Theft of physical assets is well above average and information theft, compounded by growing IT complexity, is also a significant risk. Even though they are aware of these dangers, Mexican companies are either less likely or only about as likely as average to invest in every anti-fraud strategy covered in the survey.

Kroll findings

LATIN AMERICA

The Latin American fraud picture is one of transition. Although the overall number of companies suffering at least one fraud declined, there has been a striking increase in companies reporting they are at risk. Companies describing themselves as at least moderately vulnerable to theft of physical assets or vendor fraud spiked 29% while others also saw notable increases. Companies in this region are investing in a range of fraud prevention strategies, including IT security, physical asset security, and financial controls.

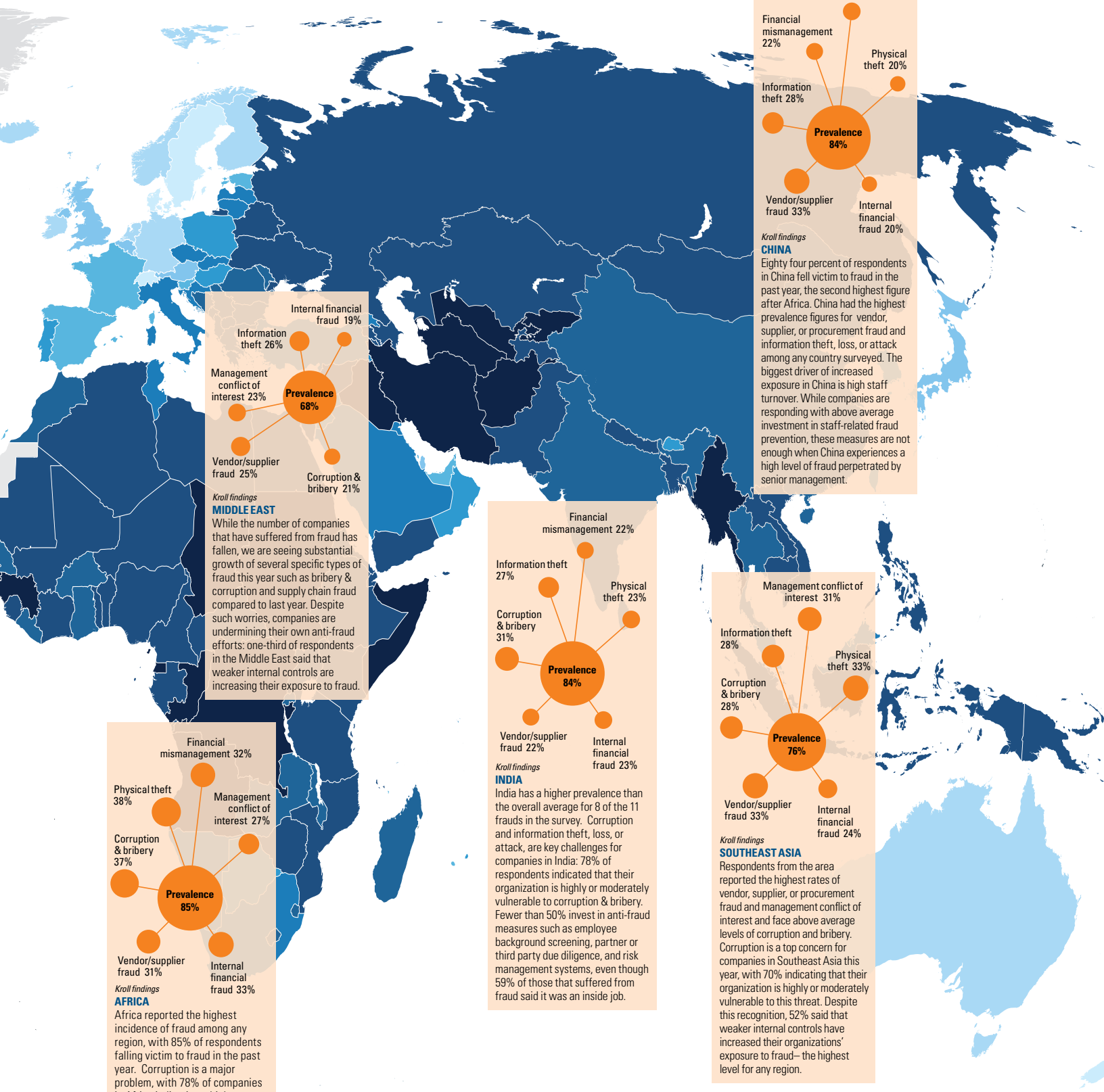
The panels on the map summarize:

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

Transparency International Corruption Perceptions Index 2009

Very Clean	9.0 - 10.0
	8.0 - 8.9
	7.0 - 7.9
	6.0 - 6.9
	5.0 - 5.9
	4.0 - 4.9
	3.0 - 3.9
	2.0 -2.9
	1.0 - 1.9
	0.0 - 0.9
Highly Corrupt	No data

Map image by permission Transparency International.
All analysis Kroll/Economist Intelligence Unit.



Kroll findings

CHINA

Eighty four percent of respondents in China fell victim to fraud in the past year, the second highest figure after Africa. China had the highest prevalence figures for vendor, supplier, or procurement fraud and information theft, loss, or attack among any country surveyed. The biggest driver of increased exposure in China is high staff turnover. While companies are responding with above average investment in staff-related fraud prevention, these measures are not enough when China experiences a high level of fraud perpetrated by senior management.

Kroll findings

MIDDLE EAST

While the number of companies that have suffered from fraud has fallen, we are seeing substantial growth of several specific types of fraud this year such as bribery & corruption and supply chain fraud compared to last year. Despite such worries, companies are undermining their own anti-fraud efforts: one-third of respondents in the Middle East said that weaker internal controls are increasing their exposure to fraud.

Kroll findings

INDIA

India has a higher prevalence than the overall average for 8 of the 11 frauds in the survey. Corruption and information theft, loss, or attack, are key challenges for companies in India: 78% of respondents indicated that their organization is highly or moderately vulnerable to corruption & bribery. Fewer than 50% invest in anti-fraud measures such as employee background screening, partner or third party due diligence, and risk management systems, even though 59% of those that suffered from fraud said it was an inside job.

Kroll findings

SOUTHEAST ASIA

Respondents from the area reported the highest rates of vendor, supplier, or procurement fraud and management conflict of interest and face above average levels of corruption and bribery. Corruption is a top concern for companies in Southeast Asia this year, with 70% indicating that their organization is highly or moderately vulnerable to this threat. Despite this recognition, 52% said that weaker internal controls have increased their organizations' exposure to fraud– the highest level for any region.

Kroll findings

AFRICA

Africa reported the highest incidence of fraud among any region, with 85% of respondents falling victim to fraud in the past year. Corruption is a major problem, with 78% of companies in Africa indicating a high or moderate vulnerability to bribery & corruption. Africa remains the region where the experience or perception of fraud has dissuaded most companies from operating. While companies in Africa widely adopt anti-fraud strategies, weaker internal controls will make them less effective.

FCPA Reform

Help Could be Coming to Those Who Help Themselves

By Jeffrey Cramer

On November 30, 2010 the United States Senate Judiciary Committee's Subcommittee on Crime and Drugs held a hearing to discuss potential changes to the Foreign Corrupt Practices Act (FCPA). Those testifying on behalf of reform argued that the FCPA, which has not been altered in 10 years, needs to be amended to allow for greater fairness in its application by the Department of Justice (DOJ). Such sentiments were echoed on June 14, 2011 when the House of Representatives Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security also examined the issue. By the time the gavel dropped on both hearings, it was clear that Congress intended to enact FCPA reforms.

Given the aggressive enforcement of the FCPA in recent years and the very small number of court cases which have clarified it, at least five potential areas are ripe for change: clarification of what constitutes a "facilitating" payment; establishment of an affirmative defense based upon a company's compliance program; a better definition of "foreign official"; limitations on successor liability; and a change in what a company has to know in order for it to be liable. These potential changes could each give businesses a better chance of avoiding FCPA problems with federal prosecutors.

Clarification of "Facilitating" Payment

Companies have justifiably been confused as to what constitutes a permissible facilitating payment under the FCPA. Whether something is a bribe, gift, or facilitating payment is subject to interpretation, often of the prosecutor assigned to the investigation. The law abhors such vagueness. Rep. James Sensenbrenner (R-WI), the House's Subcommittee's Chairman stated that "everybody has a right to know what's illegal, and there has to be much more certainty in the law." The DOJ does give examples on its website of what constitutes a bribe as opposed to a facilitating payment, but these do not provide the necessary level of confidence as to what is proper. Statutory changes could deliver the clarity companies require to conduct their business overseas with assurance.

Affirmative Defense for a Compliance Program

This reform could have the most impact as it would afford companies a statutory opportunity to help themselves before they get into potential trouble. Similar to the "adequate procedures" defense in the UK Bribery Act, the reform might afford a company potential defenses if it showed that it had procedures in place to prevent and detect unlawful conduct. An employee acting independently might not subject the company to criminal liability if he or she circumvented the existing and reasonable compliance program. Such a reform would likely result in companies taking a more aggressive approach to compliance in order to ensure they have a sufficient program and due diligence procedures in place. Congress could make the existence of adequate arrangements a complete defense to prosecution, or it could merely codify benefits such as lesser penalties in order to encourage companies to investigate violations on their own and self-report to the DOJ or the Securities and Exchange Commission.

Clearer Definition of "Foreign Official"

If there is one term in the FCPA that confuses more than "facilitating payment," it is "foreign official." Under the Act, "foreign official" is defined to include any officer or employee of a foreign government or any "instrumentality" thereof. The current

language makes it difficult for businesses to determine if they are risking a violation of the law when they do transactions with partially government-owned entities. Trying to establish what constitutes an "instrumentality" is nearly impossible in some parts of the world where governments own a portion of many firms. Changes to the FCPA may provide clearer direction to business in the form of examining the percentage a foreign government owns of a subject firm or similar test.

Limitation of Successor Liability

The FCPA could be amended to eliminate or limit the liability of an acquiring company if a pre-purchase FCPA violation by the acquired company surfaces. Such a benefit might be derived only if the acquiring firm discloses and remedies the conduct by an investigation of the acquired company, making a robust due diligence and internal audit all the more attractive for the acquiring business.

Limitation of Liability to Willful Violations

For all but some minor criminal offenses, mens rea – Latin for guilty mind – is basic to establishing the guilt of a defendant in committing a crime. The FCPA requires that individuals accused of violating the Act do so "willfully." Companies, however, could be held criminally liable if they were merely aware of the relevant criminal acts but failed to remedy them. Strict liability in this context could result in problems for a company if the person who violated the FCPA was an employee at the time of the crime. It makes sense for the individual mens rea requirement to be the same as that which would expose a company to liability. Without this change, businesses will continue to be subject to prosecution even if they were unaware of the violation by an employee until after the fact. This potential reform is crucial when analyzing corrupt payments to foreign officials which are routed through agents or other third parties. There may be a carve-out for higher level executives whose actions, it can be argued, are more closely tied to the company's fate.

After the June 2011 hearing, Rep. Sensenbrenner informed those present that the Subcommittee would start drafting legislation and told the DOJ representative that the Department should "get the message." Companies looking to limit their FCPA exposure should take heed as well. Regardless of which reforms pass, companies that are subject to regulation under the FCPA should take affirmative steps to protect themselves. These steps should include appropriate levels of due diligence, training and monitoring. This will put companies in a position to help themselves.

Jeffrey Cramer is a managing director and head of Kroll's Chicago office. Since joining Kroll, he has worked with companies to draft their compliance plans and lead due diligence investigations into foreign intermediaries throughout the world. He was previously a prosecutor in New York and Chicago and has investigated several FCPA cases during his 13 years in law enforcement. Most recently he was a Senior Litigation Counsel for the Department of Justice in Chicago.

Investing in the BRICs

Extra due diligence is vital

By David Holley and Doug Frantz

The fertile and fast-growing economies of the BRIC (Brazil, Russia, India, and China) countries are calling to international corporations, investment banks, and investors like the Sirens sang to Jason and his shipmates in Argonautica. The haste to take advantage of these burgeoning markets can lead to rushed decisions, shortcuts in diligence, and potentially unmeasured business decisions. Whether a company is entering a new market, contemplating a joint venture with an overseas partner, investing in a foreign business, or acquiring an overseas company, an appropriate level of due diligence on the foreign entity, its agents, business partners, and intermediaries is required to avoid problems associated with current anti-bribery legislation. However, the results of the 2011 Global Fraud Survey indicate that fewer than one in four respondents believe that their due diligence is sufficient to fully understand whether the acquisition target complies with either the United Kingdom Bribery Act (UKBA) or the United States Foreign Corrupt Practices Act (FCPA). In addition, nearly one out of two respondents consider their companies to be moderately to highly vulnerable to corruption, which is among the leading reasons why companies avoid investing in new regions or countries.

The high level of concern uncovered in the survey may overestimate the true degree of compliance because companies often believe they are doing better in following the law than they are actually are. Even if we accept these self-reported estimates, however, there is cause for alarm over the exposure of many corporations to the criminal sanctions and costs imposed by the FCPA and UKBA, particularly in this era of aggressive enforcement by the Department of Justice (DOJ) and Britain's Serious Fraud Office (SFO), respectively. The question then becomes what steps should be taken by a corporation determined to follow the spirit and letter of the law. Managing the anti-bribery risks through heightened due diligence should be a paramount focus when expanding into the BRIC markets and other emerging economies.

There is little guidance in either law as to what constitutes sufficient due diligence. The FCPA makes no mention of the term. The DOJ in "Opinion Procedure Release 08-01" has defined a "reasonable" due diligence file as containing the following: an independent investigative report by a reputable

international investigative firm; guidance by a foreign business consultant to help navigate the due diligence in the foreign jurisdiction; reports from the US Commercial Service within the Department of Commerce; the results of various databases and watch lists, DNDB, etc.; meeting notes from discussions with the US Embassy in the foreign jurisdiction; a report by outside counsel on the target; a report on the target company by an independent forensic accounting firm; and an opinion by a second outside counsel who reviewed the sufficiency of the entire due diligence process.

While the UKBA and SFO provide some direction on due diligence, they also provide a defense for companies that have adequate procedures in place to prevent the type of conduct that would otherwise give rise to prosecution. The Ministry of Justice provides some guidance on "adequate procedures" indicating that due diligence should be conducted on parties performing services for, or on behalf of, a business and that it should be "proportionate and risk-based." With relatively little guidance, it is no wonder that there is so much concern around the adequacy of due diligence undertaken in advance of a business transaction.

Assuming that multi-national corporations are doing some level of due diligence consistent with the guidance offered by American and British regulators, the question as to why the level of anxiety in respondents over the sufficiency of their due diligence remains high. When undertaking due diligence in contemplation of expansion into the BRIC and other emerging markets, consider the following recommendations:

1. The volume of publicly available information varies from country to country and is generally considerably less than what is available, for example, in the United States. In addition, the information is frequently not as well organized or as readily searchable as in many jurisdictions. This highlights the importance of "feet on the ground" and the ability to undertake discreet source inquiries to fully understand a due diligence subject.

2. The potential for encountering a Politically Exposed Person (PEP) is generally greater in Russia and China than in many other parts of the world. This requires more extensive due diligence on officers, directors, and shareholders than normal to steer clear of violations. An examination of a target's vendors and agents to ensure arm's-length transactions with unrelated parties is also recommended.

3. Media searches may not be as thorough, complete, and reliable as in other jurisdictions, as the local media and press are generally less aggressive and less likely to present an in-depth examination of issues. For instance, in countries like China and Russia, both hotbeds of recent and future M&A activity by Western companies, the simple act of checking available media outlets for information about a potential partner is likely to yield incomplete results at best. This is particularly true in China, where the tradition of an open press is weak and corruption is generally regarded as high.

4. There continues to be an absence of strong anti-corruption laws and enforcement in BRIC countries compared to the United States, the United Kingdom, and other countries. This requires a company to engage in more extensive examinations of acquisition targets' policies, procedures, and employee handbooks relating to corruption, anti-bribery, and gifts and entertainment expenditures.

Understanding the requirements of thorough due diligence is an important step, but problems can also arise when issues turned up in a review are not managed effectively. This point was driven home by the March 2011 settlement involving Ball Corporation, a US manufacturer of metal packaging for food, beverages, and household products. In March 2006, Ball acquired an Argentine entity, Formametal S.A. The Securities and Exchange Commission (SEC) found that during the course of Ball's pre-acquisition due diligence, information suggested that "Formametal officials may have previously authorized questionable payments" disguised within the company's books and records. Unfortunately, Formametal executives did not do enough to prevent further improper payments to Argentine customs officials, giving rise to the SEC's case. The SEC noted that Ball Corporation did not promptly terminate the responsible employees when company accountants learned about the improper payments in February 2007. Still, Ball's fine was a relatively small $300,000 because of the company's other remedial efforts, voluntary disclosure of the misconduct, and cooperation in connection with a related investigation.

The BRIC economies are enormously attractive investment opportunities. Estimates are that as much as 60 percent of the world's GDP will come from them by 2030. Participating in the world's fastest-growing economies carries growing risks, too. American, British, and multinational corporations need to understand the potential corruption dangers in the BRIC and similar emerging economies and undertake effective due diligence to avoid running afoul of anti-corruption laws. Certainly the DOJ, SEC, and Britain's Serious Fraud Office have recognized the risks and stepped up their scrutiny of activities in these countries as part of the overall trend in rising enforcement of anti-corruption laws globally.

David A. Holley is a senior managing director and the head of Kroll's Boston office. Since joining Kroll in 2000, David has led investigations into violations of the FCPA, and matters involving environmental contamination, internal fraud, and white-collar crime. Prior to joining Kroll, David worked for a mid-sized investigative firm and the Environmental Enforcement Section of the US Department of Justice.

Doug Frantz, a Kroll managing director in Washington, is a former Pulitzer Prize-winning investigative reporter and former deputy staff director and chief investigator of the U.S. Senate Foreign Relations Committee.

Recovering Sovereign Assets

By Daniel E. Karson

As the search for Colonel Moammar Gadhafi intensified after Tripoli fell to rebel forces in late August, so too did the discussion of how to determine whether Gadhafi and his family diverted Libyan assets to personal use and, as with other former heads of state, held moneys in secret overseas bank accounts. The US, UK and other governments had already frozen billions of dollars in bank and real estate assets tied to the Gadhafi regime, most of which will be released to Libya's new government. But what of the other assets Gadhafi may have converted?

With each new uprising across North Africa and the Middle East comes the inevitable challenge of recovering hidden assets that rightfully belong to the people. Like Gadhafi, Tunisia's deposed leader Zine al-Abedine Ben Ali and Egypt's ex-president Hosni Mubarak are also alleged to have accumulated massive fortunes concealed in bank accounts and other financial and real assets around the world.

The situation is not without precedent. In 1986, the Reagan administration evicted Ferdinand and Imelda Marcos from the Philippines after a sham election and the assassination of their chief political opponent. The same year, the US and French governments sent Haiti's Jean Claude Duvalier and his wife into exile in France. Duvalier and the Marcoses had acquired great wealth for themselves and their families while in power; assets which they secreted outside their countries in the face of widespread poverty and unemployment at home. Similar allegations were made against other dictators and political leaders, such as Asif Ali Zardari, the current president of Pakistan and husband of former prime minister Benazir Bhutto, Indonesian president Suharto and his clan during his 30-year reign, and Liberian president Charles Taylor, among others.

The notion that a sovereign has ownership rights to a country and its treasury is not a new one. The vast "crown estates" taken in the Norman conquests, much of which are still owned by the Queen of England, attest to that. But a republican form of government accords no such privilege to a head of state. And yet despots like the Marcoses, the Duvaliers and, allegedly, the Gadhafis were able to control commerce and divert state funds through a combination of raw political power, terror, and, in some cases, the support of other nations.

Of course, ill-gotten gains carry their own risks. Chief among these is that a successor government can seize assets within its borders. For this reason, heads of state must park their fortunes outside their home countries.

How do politicians export their assets? For a head of state, it's easy to do. When the depositor is a national leader or a top government official, represented by a prominent local law firm or investment advisor, and the amounts are in the seven and eight digits or more, the money does its own talking.

Governments and banks have cracked down on "no-questions-asked" accounts in many traditional flight capital havens, such as Switzerland. However, the "Know Your

Customer" policies ostensibly in effect in major banking centers are not airtight and they postdate the establishment of many suspect accounts. This was certainly so in the case of Jean Claude Duvalier, where a year ago the Swiss Federal Supreme Court upheld his claim to a $4.8 million account. (The account is still frozen.)

Over the last 25 years, successor governments and opposition political parties have tried to track down the assets of politicians and their families, who skimmed money off government contracts or, as the Duvaliers did, simply wrote checks to themselves out of the national treasury.

The plunder goes on today and, not surprisingly, it is poor nations that are being ransacked. The good news is that the Tunisians, Egyptians and Libyans will have an easier time tracing and recovering assets than did the Philippine and Haitian governments, if they can prove their cases against their former rulers. Mutual assistance treaties and the worldwide media attention focused on the excesses of deposed rulers have unlocked the vaults, if not the hearts, of the Swiss and other governments.

The Trappings of Wealth

Heads of state and their spouses spend their countries' wealth not unlike the "ordinary" very rich. They buy real estate (the Marcoses) and jewelry (the Duvaliers). They support entourages (Charles Taylor). And, of course, they open foreign bank accounts (all of them.)

There are two keys to unlocking the secrets: records and human sources. The first is simple enough, and falls into two categories – personal records and public records. Investigators can usually make a quick score and identify assets by getting their hands on the records all heads of state leave behind in some form or another. In addition, since egomaniacs rarely contemplated being out of power, they often have acquired assets located in countries where business registrations and property records are public and reveal personal holdings. Within 90 days, depending on what records have been left behind, investigators usually are able to find some bank accounts, businesses, properties, airplanes and yachts. These findings often lead to other assets as well. The Marcoses owned office buildings in Manhattan, thinly disguised behind a corporation in Curacao. Iraq's former president Saddam Hussein controlled corporations in the US and the UK, nominally headed by former government ministers.

The Duvaliers simply wrote checks to themselves off bank accounts in their own names. Charles Taylor's (Liberia) family held title to deeds to properties in Florida in their own names.

The next key to unlocking assets is to interview the people in the know. When dictators depart, they leave behind cadres of aides and functionaries, who did the drudge work of keeping records and running errands. Many of those who did not get a ticket out face jail sentences for complicity in the larceny. They have an incentive to "work off" their time by disgorging intelligence on assets and asset locations. It is important to get to these people early in the process. They may have records which become road maps to the assets.

Where are the assets of the most recently deposed heads of state? It is a fair guess that anyone who came to power before it became unpopular to be a flight capital haven parked their cash in Switzerland, The Channel Islands and Liechtenstein. These were rock-solid, secure places with official "no-tell" policies. Gadhafi and Mubarak would fall into this category.

However, beginning with the Marcos and Duvalier cases, Swiss banks and the Swiss government found themselves burdened with endless litigation and terrible press. They went from being seen as a secure and discreet banker to the wealthy to a protector of tyrants and murderers. As a result, the Swiss began to cooperate with successor governments. Apparently without prompting, they froze the bank accounts of Tunisia's Ben Ali on their own initiative. Separately, the agreement by UBS to turn over to the US government the names of American account holders also evidenced a transparency never before seen in that country.

As the customary flight capital havens have crumbled or at least thinned their shrouds, times have gotten tougher for larcenous dictators.

First, many countries have pledged support to one another through Mutual Legal Assistance Treaties. Under these treaties, governments will provide assistance (in varying degrees and with many exceptions) to law enforcement and tax collection agencies of other governments. A search for a former head of state's assets can fall within the scope of a MLAT.

Second, every day we become more record-intensive societies. While the accumulation and storage of business and personal data is greatest in the developed world, the rest of the world is slowly catching up. More and more information can be identified through databases, making it harder to conceal beneficial ownership, among other asset indicators.

Third, as with Switzerland, the tide of public and political sentiment has turned against offering safe havens to deposed dictators. Former heads of state may find refuge outside their country or safe passage to internal exile within, but they are almost certain to lose any court battle over excessive wealth that can be tied to them.

However, serious challenges remain. MLATs with The Cayman Islands and other Caribbean nations do not automatically ensure that governments will open their books if the alleged crime is not recognized in their countries. This includes tax violations, a customary leverage point for asset investigations.

Also, political relationships may influence a country's decision to cooperate with an asset investigation. A former head of state – Gadhafi is a good example – may have cultivated warm relations with other oppressive regimes that might serve him in exile, as a haven for both himself and his cash. Hugo Chavez, who is very much still in power in Venezuela, is in the process of moving Venezuelan gold bullion from the United States to Russia, China and Brazil. He is being treated for cancer; his country is rife with violent crime, power shortages and other problems. If Chavez is defeated at the polls, his relations with these countries may serve as a down payment for his retirement home.

Central banks and regulators can and should prohibit their member institutions from establishing bank accounts for heads of governments outside their homeland without establishing legitimate prior title to the assets and legal authority to transfer money. Banks also can step up the level of due diligence checks on their depositors.

By adopting such policies, in addition to implementing tough anti-bribery statutes, the world community can make it harder for tyrants to turn a nation's assets into personal plunder.

Daniel E. Karson is Chairman of Kroll Americas based in New York. He conducted the asset search investigations of the Marcoses for the US House of Representatives; the Duvaliers for the Republic of Haiti; Saddam Hussein, for the Kingdom of Kuwait; and many similar cases around the world.

NORTH AMERICA OVERVIEW

As in previous years, North America fares well on many fraud-related issues. It registered the lowest average fraud loss for any region, as well as the lowest regional incidence for five of the frauds covered in the survey: management conflict of interest with 15% of companies reporting they were affected; internal financial fraud (13%); vendor, supplier, or procurement fraud (12%); corruption and bribery (7%); and market collusion (6%). In addition, unlike elsewhere in the world, North America did not post dramatic increases in other types of fraud.

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	66%	87%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Information theft, loss, or attack (26%) Theft of physical assets or stock (23%) Management conflict of interest (15%)	Information theft, loss, or attack (32%) Theft of physical assets or stock (27%) Management conflict of interest (14%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Information theft, loss, or attack (51%) IP theft (39%) Theft of physical assets or stock (36%)	Financial mismanagement (36%) Information theft, loss, or attack (34%) Theft of physical assets or stock (31%)
Increase in Exposure: Companies where exposure to fraud has increased	79%	66%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (35%)	IT complexity (26%)
Loss: Average percentage of revenue lost to fraud	1.7%	Not available

There are, however, two particular weak spots for North American respondents. The first comes as no surprise: information theft, loss, or attack remains the most common fraud in the region, affecting 26% of companies this year. This is also the area where respondents perceive the greatest risk. A full 15% see themselves as highly vulnerable – nearly double last year's figure – and an additional 36% say that they are at least moderately vulnerable. Similarly, 35% of North American respondents point to IT complexity as the leading driver of increased exposure to risk, well up from last year's number (26%), and one of the reasons why so many more companies see their exposure to fraud growing.

Less recognized is the difficulty that companies in North America are facing with the theft of intellectual property. With 14% of companies affected – up from 10% last year – North America has the highest regional incidence of IP theft in this year's survey. Local respondents, however, have been slow to adjust to the shift. Although 39% see themselves as moderately to highly vulnerable, this figure is slightly less than the survey average (40%).

Despite noteworthy decreases in several types of fraud, North American companies will need to remain vigilant in their efforts to prevent information theft and IP theft.

When Fraud is an Inside Job

FIVE STEPS TO CONSIDER

By Richard Plansky

Fraud remains a large and growing concern for virtually every type of company in every part of the world. This is one of the conclusions of Kroll's 2011/2012 Global Fraud Survey. Another is that a large majority of frauds are committed by insiders. To be precise, 60% of frauds, in which the perpetrator is known, are committed by senior managers, junior employees, or third party agents or intermediaries – up from 55% in the 2010/2011 survey. The phenomenon of fraud as an inside job is not only prevalent but on the rise. The question is, "why?"

While there is no simple answer, it appears that the increasing fraud risk posed by insiders is, at least partially, a reflection of our information-based economy. More and more, the value of a company is not measured in tangible property – rather, it is measured in ideas. Those ideas – a company's intellectual property – tend to reside on computers and servers in the form of digital data. As a result, insiders have access to a far greater range of valuable assets – and can acquire them with far greater ease – than ever before.

In light of these trends, it is increasingly likely that companies will at some point encounter the need to investigate a fraud allegation against an insider. When that day comes, critical choices must be made that can have significant impact on the company's reputation, business continuity, and even employee morale. To that end, there are five basic steps that should be considered:

» **Lock down evidence**. When an investigation involves insiders, the need to preserve potentially relevant evidence is particularly acute. Inside fraudsters will likely have unfettered access to the materials that prove their fraud. At the earliest opportunity, steps should be taken to lock down electronic evidence that is easily destroyed. The company should be prepared to discreetly acquire forensic images of computers, taking "snapshots" of relevant accounts from e-mail servers and shared drives, preserving logs that show access to the Internet and internal IT systems, and removing relevant back-up tapes from rotation. In some cases, it may also be necessary to secure company landline

and cell phone records, access card logs, and surveillance videos.

» **Get smart discreetly**. Investigative steps can be taken at the outset to shed light on insider allegations without alerting the perpetrator. In virtually any case, a review of company e-mails and Internet browsing history will shed significant light on an insider's activities and associations, both in and outside of the office. In a case involving kickbacks or conflict of interest, a review of records showing purchases from vendors may reveal patterns and recent changes indicative of corruption. A review of corporate filings might show an ownership interest in one or more vendors, whose share of business has been increased by the insider.

» **Look for personal events that may trigger the 'need' to commit fraud**. Fraud is often sparked and/or evidenced by specific events. When an insider is suspected, it is always advisable to mine publicly-available sources for signs of financial distress like bankruptcies, recently filed litigation, divorces, judgments, liens, and large purchases that are inconsistent with the insider's known income.

» **Monitor key activities**. Consistent with corporate policy and applicable law, an insider suspected of wrongdoing should be monitored in order to develop evidence of wrongdoing and mitigate ongoing harm. Examples of potentially fruitful activities to monitor include e-mail communication on the company domain, hiring decisions, and payment authorizations made by the insider, as well as postings on social networking sites.

» **Have a succession plan**. As an investigation progresses and it appears that insider allegations are substantiated, it is important to plan for what will happen "the day after." Failure to have a succession plan can lead to delay in terminating a corrupt employee and possibly create significant business disruptions.

While every case is different, thinking through the basic steps outlined above can help companies respond ethically and effectively to the rising threat of insider fraud.

Richard Plansky is a senior managing director and head of Kroll's New York office. With 19 years of investigative and law enforcement experience, Richard manages a wide variety of complex assignments with a special emphasis on corporate investigations.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **TECHNOLOGY, MEDIA & TELECOMS**

The technology, media, and telecommunications sector had a mixed fraud picture over the last year. Although it experienced a noticeable decline in fraud prevalence overall, particularly for information theft (dropping from 37% to 29%) and IP theft (from 27% to 22%), it still had the highest prevalence of these two frauds of any industry. For IP theft, this was the second year in a row it held this dubious distinction. Sector companies understand that this is a problem: they are the most likely of any industry to consider themselves highly or moderately vulnerable to information theft (59%) and IP theft (49%). Moreover, certain other frauds are increasingly common in the sector: procurement fraud hit 21% of firms (up from 15% last year), financial mismanagement 16% (up from 10%), and corruption 11% (up from 7%).

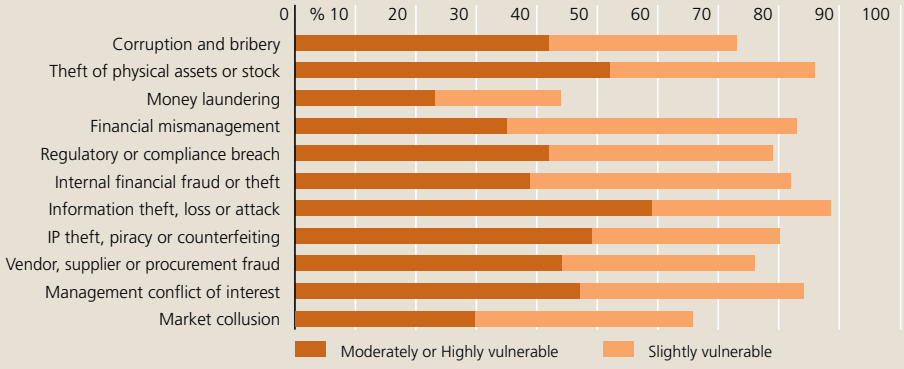
Loss: Average percentage of revenue lost to fraud: 2.1%

Prevalence: Companies affected by fraud: 74%

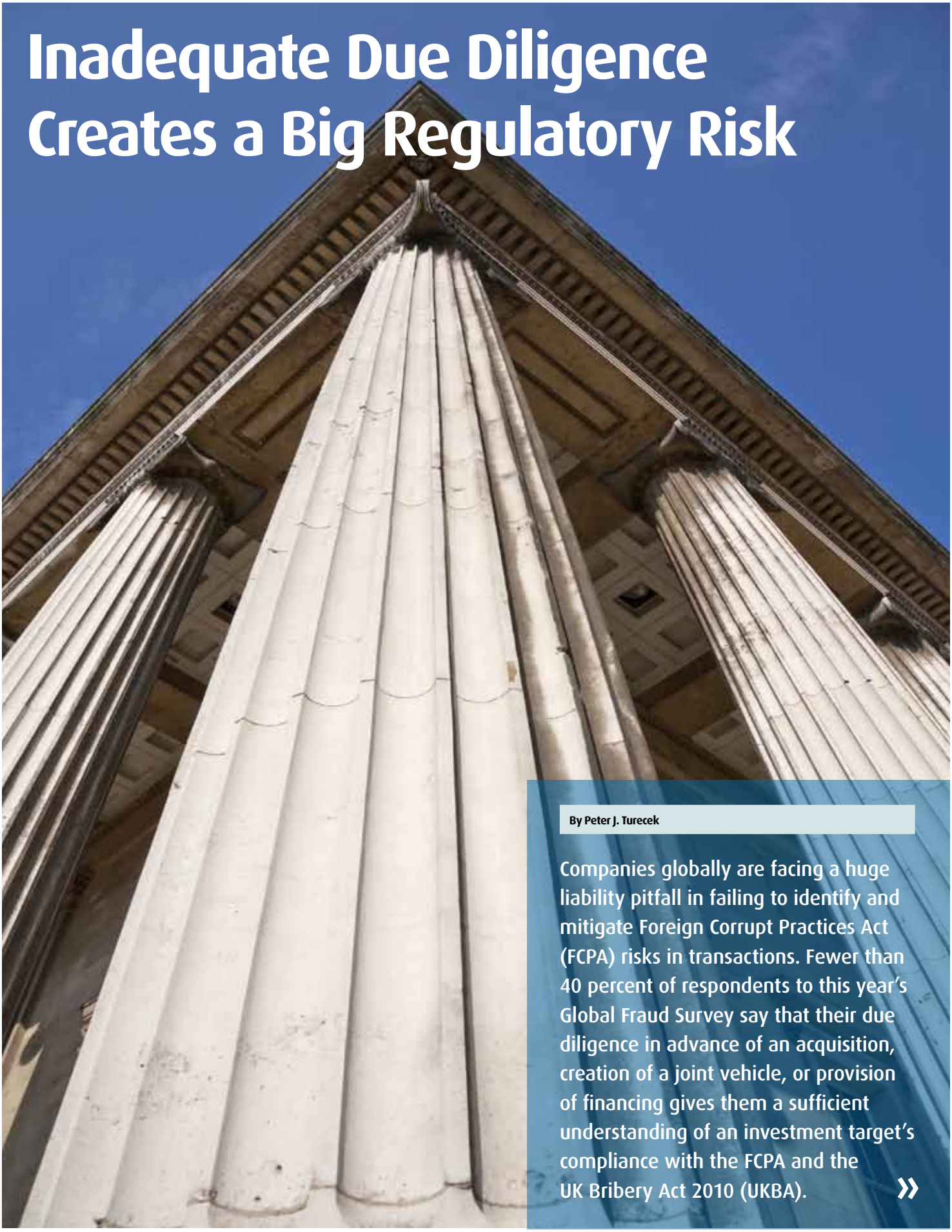
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud
Information theft, loss or attack (29%) • Theft of physical assets or stock (24%)
Management conflict of interest (23%) • IP theft, piracy or counterfeiting (22%)
Vendor, supplier or procurement fraud (21%) • Internal financial fraud or theft (18%)
Financial mismanagement (16%)

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: IT complexity (43%)



Inadequate Due Diligence Creates a Big Regulatory Risk



By Peter J. Turecek

Companies globally are facing a huge liability pitfall in failing to identify and mitigate Foreign Corrupt Practices Act (FCPA) risks in transactions. Fewer than 40 percent of respondents to this year's Global Fraud Survey say that their due diligence in advance of an acquisition, creation of a joint vehicle, or provision of financing gives them a sufficient understanding of an investment target's compliance with the FCPA and the UK Bribery Act 2010 (UKBA). »

The cost of insufficient due diligence can be very high. In just the last year and a half, the fines and other payments associated with some FCPA settlements to end regulatory action have exceeded $200 million each, including those of BAE Systems ($400 million), Snamprogetti Netherlands BV ($365 million), and Technip SA ($338 million). Smaller settlements still involve significant expense. For example, Alliance One – a tobacco company formed by the merger in 2005 of DIMON Incorporated and Standard Commercial – was sued last year by the Securities and Exchange Commission over bribes DIMON was alleged to have paid between 2000 and 2004 to Thai government officials. To settle that civil case, Alliance consented to a permanent injunction against future violations of the FCPA, disgorgement of $10 million in profits, and retention of an independent monitor. To resolve the associated Department of Justice criminal case, Alliance agreed to pay an additional $9.45 million as a criminal fine.

Such settlements reflect only a part of the true costs of an FCPA violation. Investigation and litigation expenses, public relations consultations, and the opportunity cost of taking senior executives away from their focus on running the business could collectively add millions of dollars to the financial impact.

With regulators globally devoting increased attention towards rooting out corruption, it is only a matter of time before more companies find themselves responding to inquiries from authorities about suspect business transactions around the globe. Even investment vehicles, previously deemed safe, now contain risks. For example, private equity firms providing active management of portfolio companies are more likely to see regulators closely examining the chain of ownership and management decision-making in order to hold more parties liable when corruption is identified.

Recognition that current due diligence efforts may not provide sufficient comfort is the first step toward taking action. Companies need to significantly enhance these efforts, particularly in jurisdictions where transparency is lacking and a certain measure of corruption is considered a normal part of doing business. This is not the place for false economy. Due diligence limited to running media, litigation, and criminal checks may be low-cost, but it is simply insufficient in many global jurisdictions and may prove fatal in the long run. Outside of the United States, the scope and availability of public records shrinks precipitously. Reliance upon such sparse – and, in certain countries, questionable – data may actually increase risk rather than mitigating it.

Enhanced due diligence efforts therefore require a combination of varied techniques. At a minimum, they should include:

- A thorough review of available public records.
- A comprehensive series of human intelligence/source inquiries of people who understand the specifics of a target company's operations and reputation.
- A thorough review of the target company's books and records, particularly with regards to cash flows and how certain expenses are recorded.
- A careful analysis of the findings in the context of the local business environment, players, and activities.

As many of the companies reaching legal settlements have found, ignorance of ongoing behavior at an acquisition target is not a valid excuse when regulators start looking at potential issues involving corruption. Thorough due diligence at the outset of a transaction can ultimately save significant money in the long run – sometimes to the tune of tens or hundreds of millions of dollars – and in certain cases can even secure the very survival of the company. The alternative is an unnecessarily risky roll of the dice with the future of the firm.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **CONSUMER GOODS**

The news for the consumer goods industry is generally good this year after worrying data in 2010. The prevalence of fraud has dropped markedly from 98% of companies being hit by at least one fraud to 73%. Certain frauds in particular have seen marked reductions in prevalence: theft of physical assets dropped from 43% to 27%, information theft from 25% to 15%, and financial mismanagement from 21% to 8%—the lowest figure for any sector. Not all the news was good, however. Procurement fraud, corruption, and internal financial fraud was more widespread across the sector. The big challenge for consumer goods companies remains staff. In cases where a company has identified a member of staff who has committed a fraud, 45% of the time in this industry the culprit is a junior employee, which is 11% higher than in any other sector. Similarly, the leading driver of increased fraud exposure is high staff turnover (27%). The industry is taking up the challenge: it has a higher proportion of companies planning to invest in staff training (39%) than in any other sector, and also has the second highest number, after financial services, putting new money into background screening (27%). Continued success will depend to a great extent on the effectiveness of such efforts.

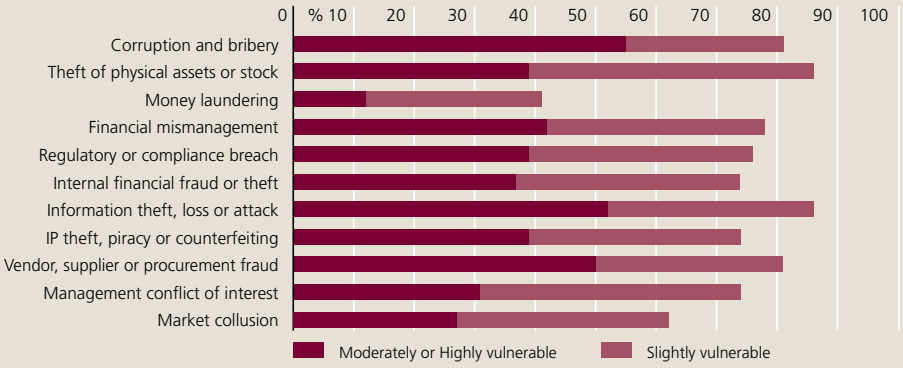
Loss: Average percentage of revenue lost to fraud: 1.8%

Prevalence: Companies affected by fraud: 73%

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud
Theft of physical assets or stock (27%) • Internal financial fraud or theft (23%)
Vendor, supplier or procurement fraud (23%) • Corruption and bribery (19%)
Information theft, loss or attack (15%)

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 (27%)



Peter Turecek is a senior managing director in Kroll's New York office. He is an authority in due diligence, multinational investigations, and hedge fund related business intelligence services. He also conducts a variety of other investigations related to asset searches, corporate contests, employee integrity, securities fraud, business intelligence, and crisis management.

Say-on-Pay in 2012

A Picture is Worth a Thousand Words

By Marcia Berss

The 2011 US proxy season has concluded, and for the first time it included "say-on-pay" – a shareholder advisory vote on executive compensation mandated by the 2010 Dodd-Frank Wall Street Reform Act.

At most companies, shareholders voted overwhelmingly to endorse executive compensation and approved pay plans with an average 90 percent support. However, at about three dozen companies, the remuneration packages were rejected, due largely to pay-for-performance concerns as reflected in weak stock prices. At more than three dozen companies, the vote passed, but with significant shareholder opposition.

The fallout has been varied. Some companies took the unprecedented step of challenging proxy advisors which advised "no" votes on executive compensation plans. One such advisor, Institutional Shareholder Services, recommended negative votes at approximately 300 companies in 2011, about 11 percent of the corporations it reviewed. A different strategy has been to fight critics by lobbying institutional investors to support proposed pay plans. Other companies altered their compensation practices before the 2011 annual meeting under the threat of a rejection. Still others have revised their compensation plans after shareholders expressed disapproval in the 2011 vote, or are considering changing executive compensation before the 2012 shareholder meeting.

Nor have shareholders been inactive. Several companies face shareholder lawsuits after failed say-on-pay votes and, in some cases, stock owners displeased with executive compensation have targeted directors who sit on the compensation committee by voting against their re-election.

In this charged environment, the 2012 proxy statements will include potent new information for shareholders: disclosures which compare executive compensation to the financial performance of the company, including dividends and changes in the stock price. The Securities and Exchange Commission is issuing rules to implement this pay-for-performance requirement, which is also part of Dodd-Frank, and may require graphic representation of the information. In the 2011 proxy season, certain companies got a jump start on this requirement and for the first time included charts in their proxy statements depicting five year total shareholder return compared to total executive compensation.

For already-disgruntled shareholders, these pictures will be worth a thousand words. However, compensation consultants and governance attorneys warn the new pay-for-performance disclosures may not accurately reflect all relevant information, such as the company's financial performance as compared to a relevant peer group, and compensation that is actually paid versus potentially earned.

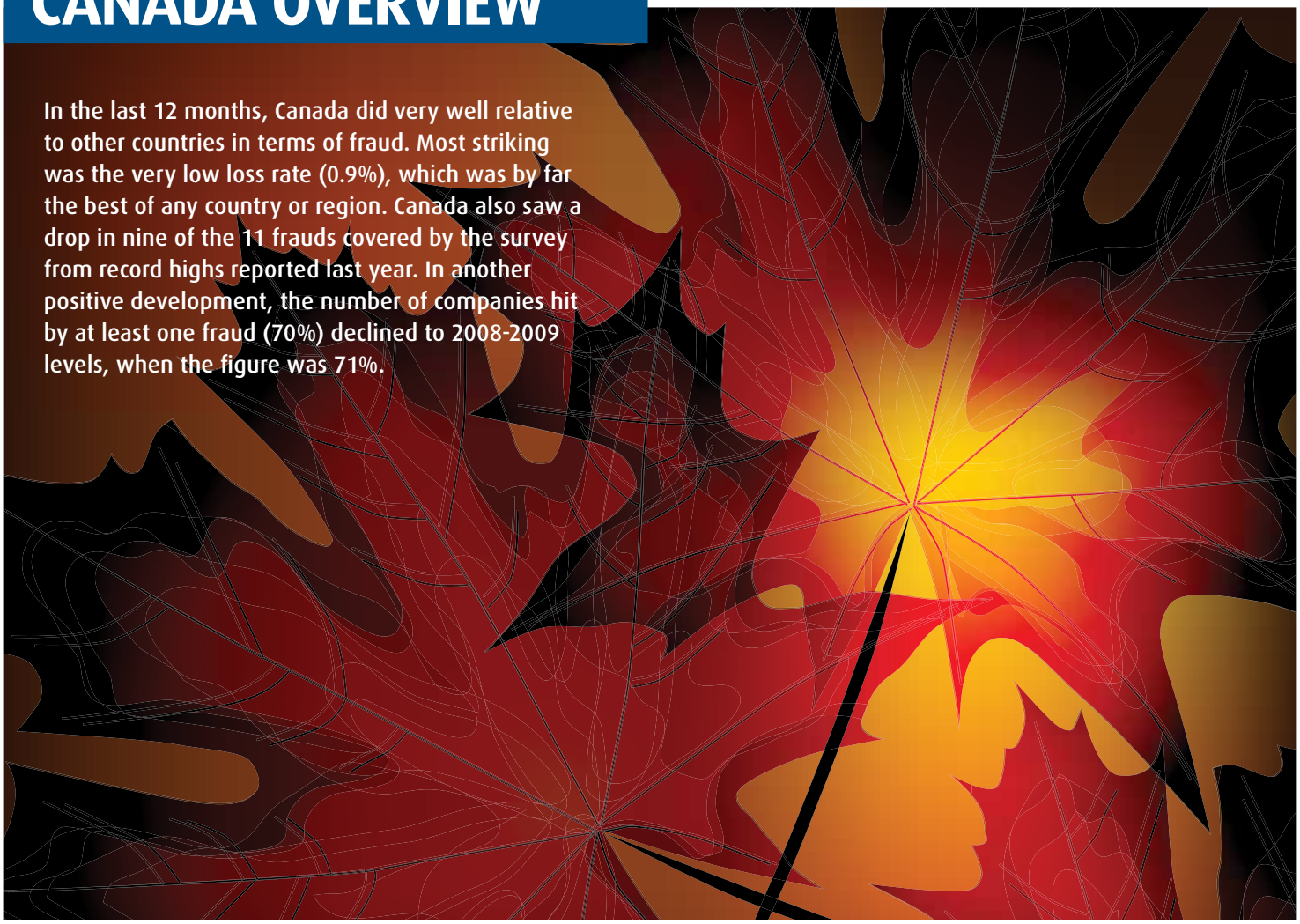
For companies receiving negative say-on-pay votes, the first step is to reach out to institutional shareholders in order to explain executive pay practices and changes, if any, to the compensation plan. The second step is to get a better understanding of the background and track record of those investors. Important information includes whether a shareholder, institutional or individual, has a history of investor activism or of working together with others as activists in a disclosed or undisclosed group – a so-called "wolf pack." Also, what are the shareholder's usual tactics? Does he, for example, have a history of launching proxy fights?

Some governance observers believe that a negative say-on-pay vote in 2011 is not worrisome, given that it was the first year in which the advisory vote was mandated. They add, though, that a second consecutive negative vote in 2012 will make the company a target for activists. It could be worse. This summer Australia revised its say-on-pay law, and now requires the board to resign if a company gets two consecutive negative votes on compensation. Simply put: two strikes and you're out.

The Dodd Frank Act has given shareholders a voice, and ammunition, to influence executive compensation. Companies are listening and need to be prepared to respond.

Marcia Berss is an associate managing director in Kroll's Chicago office specializing in public securities filings, corporate finance and corporate governance issues. She began her career as a corporate finance associate with Warburg Paribas Becker and was vice president in M&A for Dean Witter Reynolds.

CANADA OVERVIEW



In the last 12 months, Canada did very well relative to other countries in terms of fraud. Most striking was the very low loss rate (0.9%), which was by far the best of any country or region. Canada also saw a drop in nine of the 11 frauds covered by the survey from record highs reported last year. In another positive development, the number of companies hit by at least one fraud (70%) declined to 2008-2009 levels, when the figure was 71%.

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	70%	86%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Information theft, loss, or attack (22%) Theft of physical assets or stock (16%)	Theft of physical assets or stock (44%) Information theft, loss, or attack (28%) Management conflict of interest (19%) Vendor, supplier, or procurement fraud (16%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Information theft, loss, or attack (47%) IP theft (35%) Theft of physical assets or stock (34%)	Information theft, loss, or attack (48%) Regulatory or compliance breach (44%) Vendor, supplier, or procurement fraud (37%)
Increase in Exposure: Companies where exposure to fraud has increased	78%	72%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (33%)	IT complexity (35%)
Loss: Average percentage of revenue lost to fraud	0.9%	Not available

On the whole, Canadian companies are also more careful than their regional counterparts. Over half (51%) have avoided operating in – or have left – a country or region because of fraud. This is much higher than the survey average of 37%. Although corruption is the main concern for Canadian respondents, (35%), they are also nearly twice as likely as the survey average to cite information theft (21%).

The only real danger in such an environment is complacency closer to home. In particular, the prevalence of information theft, loss, or attack in the country is about the same as the global survey average (22% compared to 23%) and IT complexity is the leading cause of increased risk exposure. Moreover, 47% of Canadian respondents indicated that they are at least moderately vulnerable to this fraud, again close to the survey average of 50%. Although they see the problem as well as anyone else, Canadians are noticeably less likely to take steps against it. Only 17% intend to invest in new IT security measures in the coming 12 months, compared to 30% overall. This disconnect suggests that the relatively benign fraud environment in Canada may lead some companies to get too comfortable.

Canada Steps Up its Anti-Corruption Efforts

By Jennie Chan, Deborah Gold, Peter McFarlane

With one of the world's largest economies, Canada has many successful multinational companies, particularly in the resource sector. Major players in this industry have long used expertise gained domestically in order to develop operations overseas. Often geology dictates that these will be in difficult operating environments and in jurisdictions, which Transparency International's Corruption Perception Index suggests have some of the world's worst corruption environments. Transparency International, however, in its most recent progress report on anti-corruption activity, castigated Canada for being the only G7 country that exhibited "little or no enforcement" against this fraud. Worse still, it has been in this category since the report was first published in 2005.

For many years, Canadian multinationals caught up in corruption – whether intentionally or inadvertently – could take some comfort in knowing that the risk of prosecution by Canadian authorities under the Corruption of Foreign Public Officials Act (CFPOA) – Canada's equivalent of the Foreign Corrupt Practices Act – was minimal. That assumption, however, is looking increasingly tenuous.

Canada enacted its legislation against foreign corruption in the 1990s along with several other OECD countries. Few or no resources, however, were allocated to enforcement. As a result, no convictions took place under the legislation until 2005 when an energy service company, Hydro-Kleen, pled guilty to bribing an American public official, a conviction which came about more through the efforts of one of the company's competitors than those of the Canadian authorities.

Only in 2008 did the Royal Canadian Mounted Police (RCMP) establish its International Anti-Corruption Unit with the specific mandate to investigate allegations of foreign bribery by Canadian individuals and companies. In June 2011, after a multi-year investigation, Niko Resources Ltd., a Canadian natural gas company, pled guilty to bribing the former Bangladeshi State Minister for Energy with gifts including a Toyota Land Cruiser worth $191,000 and a $5,000 non-business trip to New York and Chicago. In addition to suffering reputational damage, the company had to pay fines totaling $9.5 million and was placed under a three-year Probation Order. The latter required Niko, among other things, to complete ongoing compliance audits to ensure its compliance with the CFPOA. The imposition of sanctions may not even be the end of this story; a new investigation concerning the activities of a Canadian Senator acting for Niko on a consulting basis is currently taking place.

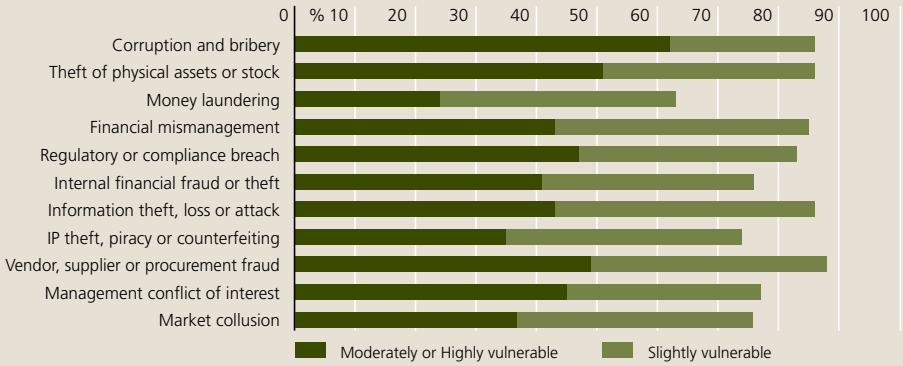
James Klotz, President of Transparency International Canada, hailed the result as "Canada's first major conviction and fine under our international anti-corruption legislation." He hopes for further action: "The new RCMP task force has been working hard at investigating Canadian companies suspected of bribery abroad… [T]here are at least 22 active files, so we expect more charges against companies or individuals." The Niko proceedings certainly do indicate that the authorities are taking a pragmatic approach to investigations and prosecutions so that these occur in a timely way. Moreover, the OECD and other bodies such as Transparency International are pressing the Canadian government to bring the CFPOA in line with legislation in other OECD countries and to increase the resources dedicated to enforcement. Such pressure also will likely mean more prosecutions under the CFPOA in the future.

Due to enhanced FCPA enforcement efforts by American authorities over the last few years, as well as the resulting significant fines for violations and transgressions concerning bribery of foreign officials, many US multinationals have implemented comprehensive programs to ensure FCPA compliance. If they have not done so already, Canadian multinationals, particularly those operating in high risk jurisdictions, should also ensure that senior management is committed to complying with the CFPOA by putting in place appropriate policies and procedures designed to detect and deter such activity. Prosecutions that may potentially result in substantial penalties are now a real risk for Canadian businesses.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **NATURAL RESOURCES**

Although the natural resources sector saw an overall decline in fraud prevalence, the industry still had the highest proportion of companies hit by fraud in the last year. It was also tied with manufacturing for the second highest increase in fraud exposure of any industry (84%). Although the prevalence of certain crimes dropped from the previous survey—notably management conflict of interest, which declined from 27% to 18%—for seven of the 11 frauds covered in the survey the number of companies affected has risen. The industry even bucked two positive trends seen in the survey as a whole. Unlike most other sectors, which saw declines, the prevalence of the theft of physical assets increased (from 28% to 33%) and that of information theft held steady with last year's figures (22%). The sector's biggest problem is corruption, which is perhaps predictable, given that its ability to choose where to extract resources is more affected by nature than by local governance. It had the highest prevalence of any industry last year (29%), and also the highest number of companies saying that they are highly or moderately vulnerable to this fraud, a remarkably high 62%.

Loss: Average percentage of revenue lost to fraud: 1.9%
Prevalence: Companies affected by fraud: 82%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud
Theft of physical assets or stock (33%) • Corruption and bribery (29%)
Vendor, supplier or procurement fraud (26%) • Information theft, loss or attack (22%)
Internal financial fraud or theft (21%) • Management conflict of interest (18%) • Financial mismanagement (17%)
Regulatory or compliance breach (16%)
Increase in Exposure: Companies where exposure to fraud has increased: 84%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (34%)



Jennie Chan is a managing director in Kroll's Toronto office, specializing in complex financial investigations. Jennie has led and participated in a wide range of assignments, including internal fraud investigations, financial reviews and litigation support matters.

Deborah Gold is a managing director with Kroll Risk and Compliance Solutions, heading up its Toronto practice. She provides due diligence solutions to support clients' commercial transactions, investments, and regulatory compliance requirements, and helps them manage legal, regulatory, financial, and reputational risk concerns.

Peter McFarlane is a managing director and head of the financial investigations team in Toronto.
With more than 20 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.

LATIN AMERICA OVERVIEW

As with some other parts of the world, the Latin American fraud picture is one of transition. This year saw a drop in the overall number of companies suffering at least one fraud to 74%, a little under the global average. At the same time, there has been a striking increase in the percentage of companies reporting that they are at risk. The proportion of respondents saying that they are at least moderately vulnerable to every fraud covered in the survey grew substantially, and in five of 11 cases at least doubled. For example, those companies describing themselves as vulnerable to the theft of physical assets jumped from 29% to 58% and those vulnerable to management conflict of interest ballooned from 26% to 53%.

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	74%	90%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (25%) Information theft, loss, or attack (24%) Vendor, supplier, or procurement fraud (23%) Corruption and bribery (23%) Management conflict of interest (21%) Internal financial fraud or theft (18%)	Information theft, loss, or attack (35%) Management conflict of interest (27%) Theft of physical assets or stock (26%) Vendor, supplier, or procurement fraud (22%) Regulatory or compliance fraud (21%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (70%) Theft of physical assets or stock (58%) Management conflict of interest (53%)	Information theft, loss, or attack (34%) Theft of physical assets or stock (29%) Management conflict of interest (26%)
Increase in Exposure: Companies where exposure to fraud has increased	79%	85%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (30%)	High staff turnover (34%) IT complexity (33%)
Loss: Average percentage of revenue lost to fraud	1.9%	Not available

This unexpected combination of lower incidence and higher perceived vulnerability probably arises from shifts in the types of fraud that companies are seeing. Although the incidence of information theft and management conflict of interest dropped (from 35% to 24% and 27% to 21% respectively), both remain troublingly common. At the same time, other frauds saw notable increases, such as internal financial fraud, which affected 18% of companies in this survey, up from just 13% last year.

Corruption, however, is the fastest growing problem. Nearly one in four companies in Latin America (23%) was affected by this crime in the last 12 months, up from 13% in last year's survey. Moreover, 70% admit to being moderately to highly vulnerable, up from just 20% last year. These numbers may have a silver lining. Experts and residents have always known that corruption is an issue in much of the region: only three of its countries finish in the best third of Transparency International's Corruption Perception Index. The results, therefore, may indicate not just a growth in corruption – although other data sources indicate that this is happening – but also a growing recognition that bribery should not be a part of normal business.

Latin America's Uneven

By Andrés Otero

At a time when the global economy is wracked by uncertainty and volatility, Latin America – led by Brazil – continues to present significant opportunities for investment and growth. The arbitrariness of its legal systems, however, and the lack of independence of the judiciary in several countries continue to be of concern to many investors and corporations operating in the region[1]. Whether it be a government expropriation of assets of an energy company, a rigged public bidding process, an environmental dispute with an indigenous community, or the alleged corruption of a high-level government official, Latin America continues to raise doubts about transparency, legality, and fairness.

For many decades, investors stood on the sidelines in Latin America because of corruption, political turmoil, lack of competitiveness, poverty and inequality, kidnapping and insecurity, terrorism, and a general lack of trust. This is no longer the case. Many foreign companies, attracted by high commodity prices and expanding local markets, are looking to the region for the first time and liking what they see. International rating agencies have granted investment-grade ratings to several countries in the region, leading to a change of perception and a larger appetite for Latin American risk. Local investment funds, as well as Latin America-based multinational companies, often referred to as multilatinas, have also increased their bets by investing and expanding in neighboring markets.

In addition to producing many of the world's highly valued food and mineral commodities, Latin American countries are updating and expanding their aging infrastructure, and governments in the region are awarding multi-million dollar contracts and long-term concessions. These opportunities have prompted many international companies to invest at a fast pace, often leaving them exposed to potentially costly disputes and legal actions. While Latin America is undeniably a more attractive business opportunity than it has been in a long time, investors need to be aware of the potential pitfalls.

What many fail to understand fully is that the rule of law in some Latin American countries is a far cry from the international standards of justice that they may be used to in developed markets. In Latin America, they will often be operating on uneven – and potentially hazardous – playing fields. Any litigation may take years to resolve, will be costly, and could potentially impact the company's global reputation and financial stability.

The main issue is the highly politicized justice system in these countries. Many high courts are composed of political appointees. Magistrates start wearing their robes owing political favors. This leads to intervention by other branches of government in judicial affairs and judgments that can favor politically connected local interests. Some judges can find themselves being pressured by interested parties or negotiating their next political assignment based on the outcome of certain cases. Transparency is often non-existent. In others, court rulings may be made in closed chambers. Under such circumstances, those with fewer connections and less knowledge of how the system operates will be at a distinct disadvantage.

Although this is especially the case in ALBA[2] countries and in most Central American nations, not all countries should be tarred with the same brush. Chile, Colombia, and Brazil, for example, have made strides in strengthening the independence of their judicial systems and higher courts, allowing very limited intervention from their governments. However, given the caudillo[3] mentality of most rulers in Latin America, there remains a constant threat to the order of justice and democracy.

While none of the above will be new to seasoned investors who have been doing business in Latin America for many years, some recent developments have added even more elements of risk for unsuspecting companies.

Playing Field

One example is class action lawsuits against multinational companies, funded by private equity firms. Some lawyers and investors are seeking to replicate the success obtained by the classic "strike suit" law firms in the United States that made billions in product liability litigation. They have targeted large multinational corporations with operations in the less developed world, bringing lawsuits on behalf of local citizens claiming personal environmental injuries, allegedly inflicted by the defendants. In some cases the causes of action have been based on the alleged conduct of predecessor companies acquired by the defendants decades earlier.

Class action fervor in the United States has been quieted to some extent by criminal convictions of lawyers and professional plaintiffs who turned fraudulent schemes into lawsuits against large corporations. However, the concept of piggybacking a contingency award on the backs of alleged mass tort victims has found a new life. In the last few years private equity firms have been created whose main investment specialty has been the funding of such actions. In many cases the founders of these firms have been former litigators themselves.

The firms operate by buying investment stakes in lawsuits. Like the class action law firms, they put up millions of dollars for legal expenses, experts and the other costs of litigation. The contracts they write vary, but essentially the longer the lawsuit goes on, and the more money they put up, the higher their return will be on an eventual judgment.

There is certainly a public benefit to contingency lawsuits. They enable injured people without means to obtain legal redress and compensation for their losses. But lost in the outwardly benign purposes of contingent fees, are those cases where indigenous and community groups who may barely understand the cause of action brought on their behalf, and ultimately may come away with a small fractional share of an award.

Multinational companies face similar challenges with government projects involving public bidding contracts. All too often in several Latin American countries, the player with the closest connections to the project wins. Frequently, the contract award is not based entirely on the lowest bid, the quality of services offered or price. The selection is often made behind closed doors without little if any transparency. This has led to unfinished infrastructure projects, litigation disputes and investigations of corruption. If a frustrated foreign bidder sues a government, the odds of succeeding or even getting a fair hearing in court are uncertain at best. After years of civil litigation a foreign plaintiff may end up seeking recourse in an international arbitration tribunal claiming that it was denied equal justice under bilateral treaty.

There are exceptions to this generalized description. To root out corruption, for example, Brazil and Chile have enacted legislation similar to the United States Foreign Corrupt Practices Act and Britain's Bribery Act. Other countries, such as Colombia and Peru, are making strong efforts to fight corruption in the public sector and to provide a sound environment for investors. Having said this, the battle against corruption is just beginning and fair play is far from becoming the standard way of doing business in the region. The results of this year's Global Fraud Survey make this point loud and clear: 70% of companies in Latin America acknowledge that they are vulnerable to corruption and bribery.

Despite the new allure of Latin America as a land of opportunity, in many countries little has been done to address the lack of an impartial system of civil justice. International investors must assess the risks associated with economic opportunities of a country before jumping in. They must also conduct thorough reputational due diligence investigations of their partners and third party agents with whom they plan to do business. Businesses and investors today are excited about Latin America, and there are compelling reasons that support this enthusiasm. Still, they should be aware that structural changes in these attractive markets are long overdue, and that political stability and impartial justice in the region are works in progress.

Andres Otero is a managing director and head of Kroll's Miami office. In addition, Andres oversees Kroll's offices in Argentina, Colombia, Mexico and Grenada and manages client relationships in the Andean region, Southern Cone, Central America and the Caribbean. He's an expert in a variety of investigative and intelligence areas, including fraud and anti-corruption services, money laundering investigations and conflict resolution matters.

1 Risk areas highlighted by the World Bank's annual Doing Business report.
2 ALBA is the Spanish-language acronym for the Bolivarian Association of Nations, an international cooperation organization currently led by Venezuelan president Hugo Chavez, members of which include Venezuela, Ecuador, Bolivia, and Nicaragua.
3 A Spanish term for a charismatic, egocentric leader who believes that his country cannot survive without him.

MEXICO OVERVIEW

This year's survey indicates that Mexico has a widespread fraud problem. Respondents posted above average incidences for eight of the 11 frauds tracked in the survey. The country also reported a slightly above average percentage of revenue lost (2.2%), which compares badly with those of its North American (1.7%) and Latin American (1.9%) neighbors.

	2010-2011*
Prevalence: Companies affected by fraud	69%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Corruption and bribery (37%) Theft of physical assets or stock (31%) Information theft, loss, or attack (27%) Internal financial fraud or theft (23%) Vendor, supplier or procurement fraud (21%) Management conflict of interest (21%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (81%) Theft of physical assets or stock (65%) Information theft, loss, or attack (58%)
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	IT Complexity (35%)
Loss: Average percentage of revenue lost to fraud	2.2%

*Insufficient respondents in 2010 to provide comparative data.

The country's biggest fraud problem is corruption and bribery. After Africa, Mexico has the second highest percentage of respondents of any region or country reporting losses in this area (with rounding, both geographies show a figure of 37%). The danger is even more widespread than the incidence: 45% report being highly vulnerable to this risk – nearly twice the survey average (24%) – with a further 36% moderately vulnerable.

The incidence of theft of physical assets (31%) is also well above the survey average (25%), and the number of those considering themselves at least moderately vulnerable (65%) is substantially higher than the figure for the survey as a whole (46%). Finally, information theft is a significant risk, compounded by the growing IT complexity.

Although Mexicans are aware of these dangers, more aggressive anti-fraud tactics than currently being adopted are probably in order. Respondents from the country were either less likely or only about as likely as average to have invested in every anti-fraud strategy covered in the survey. More striking still, except for protection of physical assets – in which 34% plan to invest in the coming year – they are also only about as likely as the average to spend more on these strategies. For information security, for example, just 26% planned to make such investments compared to 30% for the survey as a whole.

Mexicans recognize that they are vulnerable to fraud. Now they need to do something more about it.

Rooting Out Fraud After Acquisitions in the Brazilian Sugar and Ethanol Industry

By Vander Giordano

The Brazilian sugar and ethanol industry has become an important option for investors seeking to increase their holdings in the energy sector. Several factors, notably the country's large sugarcane production, the instability of global oil prices, and growing worldwide concern over the environmental impact of energy production, have combined to make the sector particularly attractive.

Brazilian government support adds to this appeal. The National Economic Development Bank has approved some $35 billion in loans to private companies in the sector over the next four years. These will support the growth of sugarcane plantations, spur technological development in the industry, and finance the expansion of ethanol distilleries, pipelines, and other transportation networks for the industry.

It is not surprising that an increased participation of foreign capital has accelerated consolidation within the sector in recent years. The transformation has been dramatic. What was once an industry of primarily family-owned businesses is now dominated by professionally run companies. This trend is expected to continue as large firms increase their market share and the number of small enterprises further diminishes.

This transformation brings a variety of challenges, including a culture shock for Brazilians as the archetypical powerful local business owner – a staple of the country's literature and political imagery – is slowly being replaced by faceless executives. International investors face other issues as well. Kroll has seen a high incidence of unethical behavior in the pre-sale phase of transactions, especially in the cases of heavily indebted sellers. These practices, including fraud and other questionable behavior by employees and suppliers may continue even after the arrival of new owners.

Once the acquisition is complete, those buying a Brazilian sugar and ethanol producer would be well advised to undertake a comprehensive internal review, with special attention to budget execution, late payment of vendors, expenses for supplies, contract enforcement and outstanding debts. Particular attention should be paid to activities involving industrial and agricultural warehousing; cutting, loading and transportation of sugar cane; delivery of farm supplies; provision of contracted services; and company fuel supplies. The most important step of all is to implement a new system of internal controls.

The following may help to minimize risks in the period after the purchase is completed:

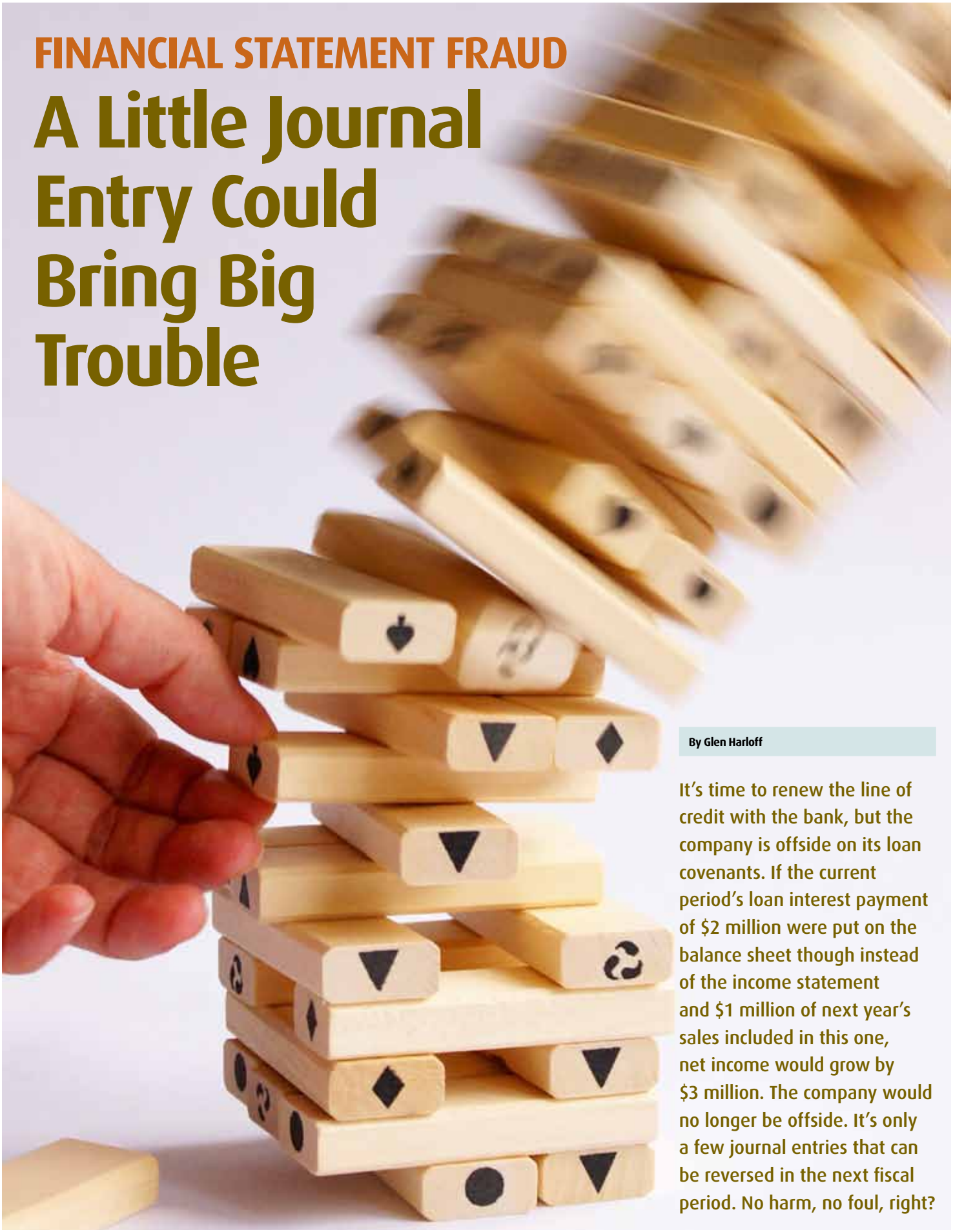
1. A good way to start the process of transforming internal procedures is to set up an effective channel for internal communication to funnel the ideas, suggestions, and complaints of employees that impending changes inevitably create. It is important to give this channel credibility by providing prompt and full responses to employees' concerns. The change of personnel in key positions at this early stage will help ensure that the company's answers are clear and objective. The human resources department will play a central role in this process.
2. The next step is a complete review of all major agricultural and industrial processes with particular emphasis on the role of each employee. A thorough review and crosscheck – using a company's Enterprise Resource Planning systems – of purchase orders, payrolls and work hours, and price curves of key inputs will provide a detailed picture of the plant's operations and the reliability of the numbers in its financial statements and other reports. The directors of the agriculture and industrial divisions will have a key role in assuring the success of this review.
3. It is recommended that the internal transformation process be accompanied by a renewed commitment to security. In the first year of the new ownership, it is crucial to undertake a thorough assessment of the corporate security structure and technical staff, followed by the implementation of state-of-the-art security systems to ensure the highest level of asset protection at the plants.
4. To raise awareness of new business practices, management may want to conduct an internal campaign by distributing manuals, explaining ethical conduct and encouraging employee engagement based on a clearly defined set of goals set by the new owners.
5. To reinforce best practices, training modules, aimed at group leaders, help reinforce the new rules of conduct and the need for commitment from all employees to the implementation of new practices. The human resources department would be responsible for coordinating this phase of the program.

The above efforts will be necessary to help effect an ideal transformation in the newly purchased company. The participation of top management and its willingness to follow through in implementing these five steps will go a long way towards bolstering the understanding of – and the support for – any new processes that the incoming administration needs to impose. If this does not happen, however, the possible losses during the transition could potentially undermine the entire investment.

Vander Giordano is a managing director in Kroll's São Paulo office. He is a member of the Brazilian and International Bar Associations and holds an MBA. Vander has extensive experience working with companies in the energy, retail, banking and airline industries.

FINANCIAL STATEMENT FRAUD

A Little Journal Entry Could Bring Big Trouble



By Glen Harloff

It's time to renew the line of credit with the bank, but the company is offside on its loan covenants. If the current period's loan interest payment of $2 million were put on the balance sheet though instead of the income statement and $1 million of next year's sales included in this one, net income would grow by $3 million. The company would no longer be offside. It's only a few journal entries that can be reversed in the next fiscal period. No harm, no foul, right?

The proper response, of course, is "wrong." This is an example of financial statement fraud – the deliberate inclusion of misleading amounts or disclosures, or the omission of pertinent ones, in order to deceive financial statement users, especially investors or creditors. It is one of the most costly of all frauds in terms of size and damage created, but also one that tends to get the least attention.

A company's financial statements may be the only window into the company's financial affairs for the average investor and sometimes for banks and other institutional investors. At the same time, the high stakes business environment in which companies operate creates a tremendous pressure on management to portray the company in the best possible light and, as a consequence, may cause the management of some companies to create fraudulent financial statements.

The forms this fraud can take are many and various [see sidebar]. Typically, it involves multiple journal entries which use different types of falsehood, making the crime more difficult to detect. A common misconception is that financial statements prepared by auditors are an insurance policy against such misconduct. Detecting fraud, though, is not a primary objective of financial statement audits. Standard sampling techniques do not – and cannot – examine every transaction.

The perpetrator of financial statement fraud is not necessarily the company itself but more commonly a group of people within it, including senior executives at the very top of leadership who have the ability to override internal controls. The motivation may be the ostensible good of the company and its stakeholders which can allow the fraudsters to rationalize their actions. For example, a fraudster could convince himself that a few 'white lies' may seem essential in order to save the company and the jobs of its employees. Alternatively, those involved may simply be seeking their own private benefit by inflating the stock price before sale, securing performance bonuses, or even concealing other illegal acts.

So what are some of the red flags of financial statement fraud?

- Unusual or large transactions recorded at the end of an accounting period or occurring with related parties.
- Unusually rapid growth or unusual profitability compared to other periods or peer companies.
- Restrictions placed on auditors or bankers in reviewing company accounting records.
- Unreasonable assumptions or estimates.
- Management dominated by a single person or small group.

When financial statement fraud occurs, investors, bankers, and others cannot properly assess the financial health of the company and make informed decisions. As those relying on the last financial statements of Enron and WorldCom before they went bankrupt can attest, the result can be substantial losses. Companies where executives engage in fraudulent activity also run a high risk of their own demise – something management should remember when tempted to make "just a few journal entries that won't hurt anyone."

Glen E. Harloff (CGA CFI) is a managing director in the Caribbean and Latin America, specializing in forensic accounting and complex financial investigations, litigation consulting, and financial due diligence. He has been involved in numerous forensic investigations relating to publicly traded and privately held companies, and domestic and offshore financial institutions. Prior to joining Kroll, he was a member of the Royal Canadian Mounted Police where he conducted complex national and international white-collar crime investigations.

Some common forms of financial statement fraud

Revenue recognition or timing schemes

- Recording future sales in the current period
- Recording fictitious or phantom sales
- Recording gross rather than net revenue
- Recording revenues of other companies when acting as a middleman or sales of products on consignment

Understating expenses

- Deferring the recording of expenses to another period or not recording them altogether
- Reporting cost of sales as a non-operating expense to improve gross margins
- Capitalizing operating expenses

Improper asset valuations

- Manipulating the value of reserves
- Failing to write-down the value of an asset when required or changing its useful life
- Manipulating estimates of fair market value

Inadequate disclosure

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **MANUFACTURING**

Despite some positive news, the overall outlook for the manufacturing industry is a cause for concern. On the plus side, the relative cost of fraud (1.8% of revenue) is lower than the survey average (21%). The prevalence of fraud has also dropped to 74%, mirroring the decline in this year's survey average. One worry is that for eight of the 11 frauds tracked by the survey, the proportion of companies hit has risen, most notably for theft of physical assets (from 25% to 34%), procurement fraud (from 23% to 30%), and management conflict of interest (from 13% to 24%), for each of which the sector now has the highest prevalence of any industry. Manufacturing companies, however, are not responding aggressively. A lower proportion than average will be investing in all but two of the anti-fraud strategies covered in the survey. In particular, staff training will see the least widespread investment of any industry, even though high staff turnover is now the leading driver of increased fraud exposure in the sector (cited by 31%).

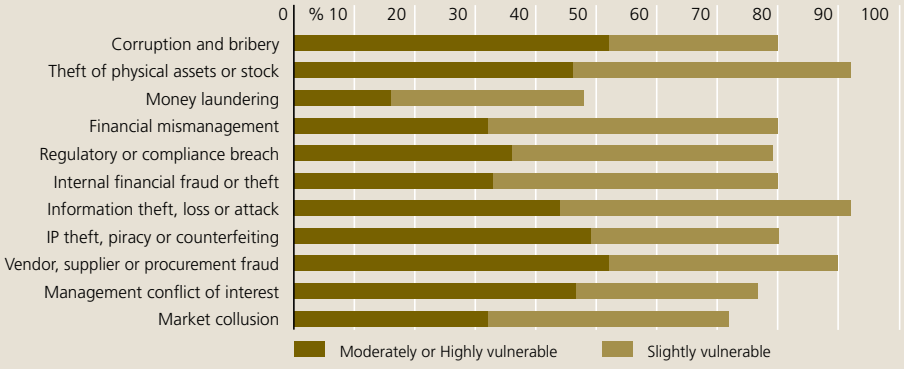
Loss: Average percentage of revenue lost to fraud: 1.8%

Prevalence: Companies affected by fraud: 74%

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 (30%)
Management conflict of interest (24%) • Corruption and bribery (21%)
Information theft, loss or attack (19%) • Financial mismanagement (17%)

Increase in Exposure: Companies where exposure to fraud has increased: 84%

Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: High staff turnover (31%)



SOUTHEAST ASIA OVERVIEW

Last year's survey showed that the developing countries of Southeast Asia had a significant fraud problem. This year the results indicate that in many ways it has grown worse.

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	76%	90%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (33%) Vendor, supplier or procurement fraud (33%) Management conflict of interest (31%) Corruption and bribery (28%) Information theft, loss, or attack (28%) Internal financial fraud or theft (24%) Financial mismanagement (21%) Regulatory or compliance breach (19%)	Theft of physical assets or stock (32%) Management conflict of interest (26%) Information theft, loss, or attack (25%) Vendor, supplier or procurement fraud (17%) IP theft (16%) Corruption & bribery (13.6%) Internal financial fraud or theft (9.9%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (70%) Theft of physical assets or stock (60%) Management conflict of interest (57%)	Theft of physical assets or stock (46%) Internal financial fraud or theft (43%) Corruption and bribery (40%)
Increase in Exposure: Companies where exposure to fraud has increased	83%	74%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	Weaker internal controls (52%)	Weaker internal controls (35%)
Loss: Average percentage of revenue lost to fraud	2.5%	Not available

While the overall incidence of fraud has declined broadly in line with the survey as a whole, the number of companies affected by nine of the 11 frauds covered has increased, with corruption and bribery, internal financial fraud, and vendor, supplier, or procurement fraud seeing the biggest jumps over last year. Southeast Asia also saw the highest incidence of any region or country for: vendor, supplier, or procurement fraud (33%); management conflict of interest (31%); regulatory or compliance breach (19%); and market collusion (14%).

Corruption is a leading concern for companies in Southeast Asia this year, with 70% indicating that their organization is highly or moderately vulnerable to this threat. This comes as no surprise given that only 14% say that their organization is well prepared to comply with anti-corruption legislation.

Despite this recognition, companies are economizing in ways that encourage fraud. Over half (52%) indicated that weakened internal controls, typically due to cost cutting, have increased their exposure to fraud in the last year – by far the highest response to this question across any region or country. Southeast Asia also had the highest number of respondents reporting that cost restraint over pay (38%) and reduced revenues (33%) had increased their organization's exposure to fraud.

If businesses in the region want to stop the spread of fraud, they need to think carefully about where they are cutting corners.

Procurement and Supply Chain Fraud in Asia

By Tadashi Kageyama and Charlie Villasenor

Vendor, supplier and procurement fraud is an increasing problem in Asia. In the recent Global Fraud Survey, a third of the respondents in both China and Southeast Asia said that they had suffered from this type of fraud in the past year. This is roughly a 50 percent increase over last year's survey.

This increase is partly due to greater awareness of existing fraud, as well as to changes in the global environment which have led to higher domestic consumption in Asia. In the past, goods were often made in China and quickly shipped out to places like Japan or the United States. The supply chain is now much more sophisticated. A good example is one Kroll client, a materials company which used to manufacture low-end chemical solutions in China and export them to other countries. It is now making more complex items in China for local consumption and hence procuring more high-end items.

The Procurement and Sourcing Institute of Asia (PASIA) believes that this shift in strategy is also focusing more attention on ethical supply management. As Asian economies grow, traditional tactical procurement and supply management processes will be challenged to drive efficiencies and eliminate gaps in compliance. Increased spending can potentially lead to a higher risk of bribery and fraud. As a result, the need for effective, efficient, and ethical procurement and supply management will be of greater importance.

Kickbacks

Supply chain fraud can take many forms, but in Kroll's experience, the most common manifestation in Asia involves kickbacks and bribery, with conflicts of interest and collusion coming second, and tender rigging being the least common. It is perhaps surprising, given the growing awareness of the far-reaching and hard-hitting United States Foreign Corrupt Practices Act, that Asian operations of well-known multinational corporations are by no means immune to this kind of fraud.

Kroll has investigated a large number of cases where the local senior manager has taken bribes from suppliers. These individuals are aware that it is against the rules – they have read the compliance manuals and signed the various documents – but they say, "Hey this goes on in the world, so why can't I do it?" In one case, an American company brought in a new general manager for its China operation. Telling the head office that it was necessary in order to obtain the best prices, the new manager called in the company's suppliers one by one and threatened to change vendors if they did not meet his requirements. In fact, he was really keeping on board those vendors who were willing to give him a kickback and firing the ones that refused to do so.

Corrupt practices are often revealed through whistle-blowing by an honest supplier, but managers can also look out for some tell-tale warning signs. One sign is a lack of thorough vendor background checks as part of the due diligence process. Some companies fall into the trap of only conducting a quick internet search on their vendors, without ever visiting their factories; often when investigators show up the vendor is not even there. Another red flag is to see one or two vendors getting all the contracts, or if the same purchaser is managing a vendor for one or two years.

Conflicts of interest

The second most common type of supply chain fraud in Asia involves conflicts of interest and collusion. In one Kroll case, a Japanese machinery company had a large operation in northern China overseen by a trusted Chinese general manager. It was only when a newly-appointed CFO carried out a management review that problems were revealed, including a significant payment to one supplier which was owned by the general manager's wife.

When confronted, the manager saw nothing wrong with his actions: in his view, he had been making money for the company and there was no real financial damage done. All the items had been delivered at fair market prices. The manager was, however, receiving a salary and dividends from his wife's company, and was clearly in breach of his employment agreement and code of conduct. In such cases, the damage is to reputation and morale. If left untended, the problem can lead to a lot more costly problems down the line.

In the procurement and supply management sector, fraud typically involves high-value items and is often committed by senior-level executives who are authorized to sign off on high-value invoices. In one case which PASIA studied, involving a foreign multinational company, a problem was only uncovered when a third-party procurement consultant was brought in to find opportunities for savings and efficiencies. He found not only opportunities but also anomalous transactions, notably a contract which had been in place for several years under terms where, although real market prices were expected to go down, the contract prices were pegged at an old, high rate without any clause to allow price redetermination.

The good news is that, due to its nature, many employees are aware of supply chain fraud. Problems can be picked up through careful vendor screening which should consist of more than a standard web search: Kroll recommends the cross-referencing of vendor information with the phone numbers and addresses of employees and their families.

As well as screening, companies need to conduct regular fraud checks at various points in the procurement cycle. This should include looking at financial data to see if there are any anomalies, such as contracts with specifications which highly favor one particular supplier. A third party procurement and supply management specialist can help identify and correct weaknesses in four areas: people, process, procurement, and governance. Such a project and its outcome must be publicly endorsed by the board and the audit committee in order to prove successful.

What the future holds

PASIA expects that, as business competition accelerates, supply chains are going to be under tremendous pressure to perform. This will also hold true for sales and business development professionals who are charged with delivering top line revenues. For both to keep themselves sustainable in the global marketplace, adherence to the highest ethical standards when buying and selling is critical.

An obvious challenge facing all countries is the absence of a global standard on ethics in procurement. This is why PASIA is offering the Global Procurement and Supply Management Ethics Certification Program, which will be rolled out in the fourth quarter of 2011. It will focus on identifying gaps in how organizations carry out their business, providing enterprise-wide education, and certifying individuals and companies in relation to sustainable ethical practices.

In PASIA's view, when you have two professionals from different countries doing business, they should establish baselines of what is ethical, and they should use global standards. Ethical practices make an organization sustainable. Ethical business is competitive. Ethical procurement and supply management is good for business.

Tadashi Kageyama is a senior managing director and head of Kroll's Asia operations including Japan. Tadashi specializes in business intelligence, investigations, and risk consulting services for corporate, financial clients and government agencies. He helps clients respond to and mitigate the risk of fraud, dispute and litigation, regulatory and compliance violations, intellectual property theft, and the theft of assets and information.

Charlie Villasenor is the Chairman of the Procurement and Sourcing Institute of Asia (PASIA) and President and CEO of TransProcure Corp. Charlie has over 20 years of experience in procurement, manufacturing and supply chain management and is on the Board for the International Federation of Purchasing & Supply Management (www.ifpsm.org).

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **HEALTHCARE, PHARMACEUTICALS & BIOTECHNOLOGY**

This was a challenging year for the healthcare, pharmaceuticals, and biotechnology sector. The good news was that, as for every other industry, the overall prevalence of fraud dropped (from 88% to 73%). The sector also saw a decline in the theft of physical assets (from 34% to 26%). The bad news, however, was that the average loss for the industry, at 2.6% of revenue, was the second highest figure for any sector, trailing only financial services, and a higher proportion of companies saw an increase in exposure (89%) than in any other industry. The problem was widespread. Eight of the 11 frauds covered in the survey saw an increase in prevalence in the last year, most notably information theft, which bucked the trend in other sectors and grew from 19% to 26%. Other substantial increases include procurement fraud (up from 11% to 23%), internal financial fraud (up from 13% to 24%), and financial mismanagement (up from 11% to 20%), which was more common in healthcare than anywhere else. Moreover, eight of the 11 frauds tracked by the survey hit more than 15% of sector companies—the sector tied with financial services for the highest number of frauds this widespread. In the past, healthcare companies have needed to focus in particular on the common threats to knowledge industries—information theft and IP theft—but now the risks are much more diverse.

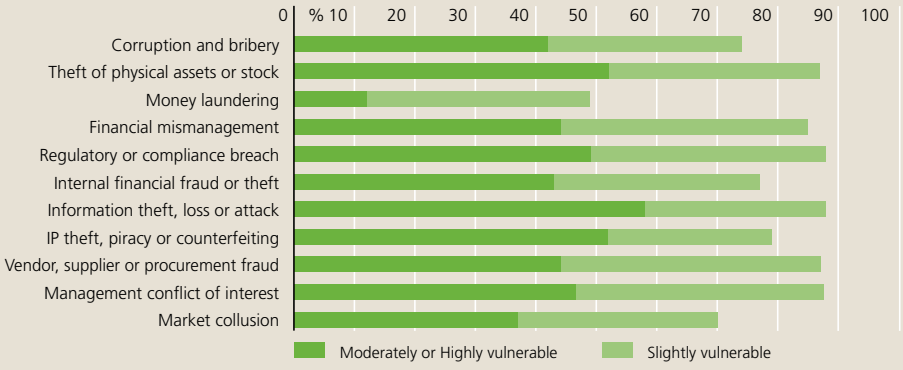
Loss: Average percentage of revenue lost to fraud: 2.6%

Prevalence: Companies affected by fraud: 73%

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud: Theft of physical assets or stock (26%) Information theft, loss or attack (26%) • Internal financial fraud or theft (24%) Vendor, supplier or procurement fraud (23%) • Management conflict of interest (23%) Financial mismanagement (20%) • Corruption and bribery (16%) • Regulatory or compliance breach (15%)

Increase in Exposure: Companies where exposure to fraud has increased: 89%

Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (30%)



CHINA OVERVIEW

China's fraud picture has improved slightly over last year, but the country still faces a tremendous challenge. Even with overall incidence declining from 98% to 84%, China still has the second-highest proportion of companies affected by fraud of any country or region, just falling below Africa's 85%. Although a number of fraud types did see marked declines, especially money laundering which dropped from last year's extraordinary figure of 20% to 1%, this may merely reflect that fraudsters are now employing different techniques.

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	84%	98%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Vendor, supplier or procurement fraud (33%) Information theft, loss, or attack (28%) Management conflict of interest (23%) Financial mismanagement (22%) Internal financial fraud or theft (20%) Theft of physical assets or stock (20%) Corruption and bribery (19%)	Management conflict of interest (30%) IP theft, piracy, or counterfeiting (26%) Theft of physical assets or stock (22%) Regulatory or compliance fraud (22%) Financial mismanagement (22%) Market collusion (22%) Corruption and bribery (20%) Vendor, supplier or procurement fraud (20%) Money laundering (20%) Information theft, loss, or attack (16%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (64%) Information theft, loss, or attack (56%) Vendor, supplier or procurement fraud (55%)	Corruption and bribery (30%) Information theft, loss, or attack (27%) Theft of physical assets or stock (26%) Financial mismanagement (26%)
Increase in Exposure: Companies where exposure to fraud has increased	84%	72%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	High staff turnover (43%)	High staff turnover (34%) Weaker internal controls (34%)
Loss: Average percentage of revenue lost to fraud	2.3%	Not available

Despite the positive news, this year's top two fraud types in China – vendor, supplier, or procurement fraud and information theft, loss, or attack – had the highest prevalence out of any country or region surveyed. The incidence of the former rose from 20% last year to 33% this year; the latter from 16% to 28%.

Eighty-four percent of respondents also report higher exposure to fraud this year – again one of the highest figures in the survey. The biggest driver is high staff turnover, one of the traditional problems of operating in China. While companies are responding with above-average investment in the coming year in staff-related fraud prevention, such as training and whistleblower hotlines (38%), these measures are not sufficient given that China had the second-highest level of fraud of any country or region perpetrated by senior management. Frauds committed by high level executives typically cost a company significantly more than those committed by junior employees, and require stronger preventative solutions.

Despite the overall drop in incidence, the sense of vulnerability to fraud in China is rising significantly. In most cases the proportion of companies where respondents reported moderate or high vulnerability has more than doubled. The top perceived risks include corruption and bribery (64% over last year's 30%), information theft (56%), and vendor, supplier or procurement fraud (55%).

THIRD PARTY VENDOR SCREENING

Compliance as a Route to a Better Business

By David Wildman

Collusion, fraud, and corruption often flourish where victims are at an information disadvantage. Due diligence may involve checking voluminous records in foreign languages and jurisdictions, so companies which rely on partners, intermediaries and agents dispersed along global supply chains face numerous vulnerabilities. Effective third party vendor screening can identify past involvement in fraud and corruption by external parties and the benefits may go further, in identifying improvements to a company's value chain. These can include culling dormant suppliers, reconciling related or affiliated companies and identifying partners whose business capacities or competencies may not actually be in line with your company's needs.

While a wide ranging forensic analysis of every business partner is obviously impractical, a failure to make reasonable and prudent inquiries about third party vendors may leave a company vulnerable to allegations of negligence and potentially liable under American, British and other countries' anti-corruption legislation. As such, a company needs a systemic program that can segment the various risks that may be inherent with various vendors, suppliers and/or partners and importantly, provide an auditable defense should a regulatory action regarding one of the vendors ever arise.

The screening needs to start with a base level review and diligence to identify red flags. Furthermore it may include consultation along a wide spectrum of multi-lingual media, Internet-based data and official records. Such information ideally should be complemented with inquiries in and knowledge of the relevant local areas, business environment, and industry circles. For example, a Kroll client recently requested checks on a Chinese company and its three principals. Research into one of the principal's uncovered two media references pertaining to bribery, committed in the same city, yet with another company. Research in court databases yielded no relevant information, but often in many jurisdictions such records are incomplete or not publicly available. Local inquiries subsequently confirmed that the principal in question had indeed been found guilty in the earlier bribery case.

Comparison and reconciliation of information provided by vendors and business partners is another important way to identify possible trouble. In addition to requesting copies of records such as company registrations or relevant licenses, compliance questionnaires should ask prospective partners and suppliers to disclose other company and business interests. Missing documents and unanswered questions are potential red flags. The checks and research can be sequenced based on key risk variables, and a more in-depth diligence can be conducted when there is a higher likelihood of exposure. In one case, Kroll established through records analysis that a person, described to our client as the legal representative and 1% shareholder of the vendor company, was in fact a 90% shareholder and legal representative of another, similar business in the same industry. Further research revealed that the companies had jointly participated in a bidding project a year earlier.

A failure to reveal interests in multiple companies that are vendors, distribution agents, suppliers, or third party agents for the same firm could be innocuous. It could also however, suggest the possibility of bid rigging, price fixing, inflated supplier costs or other opaque, non-competitive behavior.

Comparison of other data such as financial and accounting records should also be areas for concern. Kroll has identified instances where the balance sheets and income statements from some companies have been inconsistent with the respective figures filed with the corporate registration records; whilst tax and financial reporting conventions in certain jurisdictions may result in variances, some of the discrepancies noted have been significant and would indicate that at least one set of records may require further clarification.

In addition to revealing red flags, vendor screening may provide sound business grounds to revisit supplier relationships or renegotiate service level, delivery times, payment schedule or warranties. In one case, Kroll identified a situation where the client's third party vendor – a supplier of medical equipment, was actually a railway industry company, which was a subsidiary of another railway operator. Although its parent company did hold a trading permit for medical equipment, it remained an obvious question whether it had the requisite expertise, customer networks and capacity to service the medical equipment the client's business needs effectively.

Prudent and reasonable vendor screening can reveal not only past instances of fraud but also that partners may not have first point access to markets, superior products, technology, or networks. As such, a robust program can both address anti-corruption, fraud and collusion risks while also identifying key areas where business partnerships and synergies may be improved.

David Wildman M.A. is a managing director based in Kroll's Singapore office. Prior to Kroll, David was a Superintendent with the Australian Federal Police and has worked in Australia and Asia. In 2006 David was invited to participate on the Hong Kong Independent Commission Against Corruption's Senior Investigator Command Course and travelled across Northeast Asia studying anti-corruption efforts with Chinese Procuratorate counterparts.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — RETAIL, WHOLESALE & DISTRIBUTION

In many ways, the fraud environment of the retail, wholesale, and distribution sector mirrors that of the survey as a whole. The overall prevalence of fraud has dropped in line with the survey average to 74%, and there has been progress on the number of companies suffering from theft of physical assets (down from 41% to 28%) and information theft (down from 26% to 14%). This, however, has been partly counterbalanced by growth in all but one of the other frauds tracked in the survey. The most notable of these are internal financial fraud, which doubled in prevalence within the sector from 13% to 26%; market collusion, which rose from 2% to 15%; and even corruption, which, despite being less widespread here than in any other industry, affected 9% of companies, up from 4%. Just as last year, the industry's big Achilles heel is a lack of attention to staff issues. It has the highest percentage of firms of any industry reporting high staff turnover (33%) and cost restraints over pay (31%) are increasing exposure to fraud. Add to that the highest number reporting weakened internal controls (29%) and it becomes clear that the sector is running a high risk.

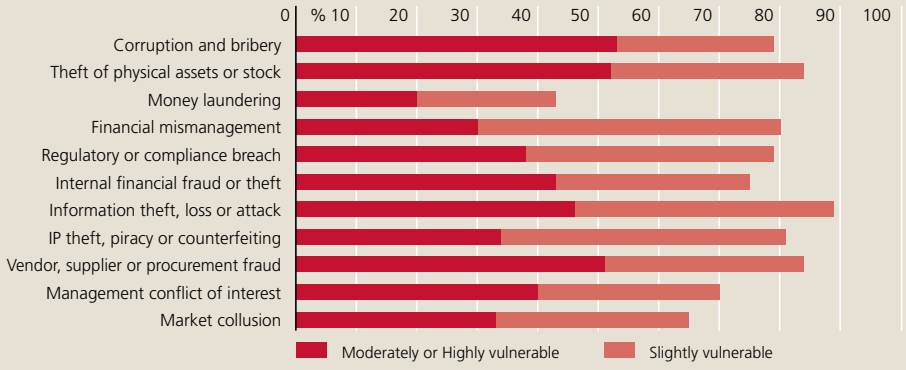
Loss: Average percentage of revenue lost to fraud: 1.9%

Prevalence: Companies affected by fraud: 74%

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud
Theft of physical assets or stock (28%) • Internal financial fraud or theft (26%)
Vendor, supplier or procurement fraud (22%) • Management conflict of interest (22%)
Market collusion (15%)

Increase in Exposure: Companies where exposure to fraud has increased: 77%

Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: High staff turnover (33%)



When A Watchdog May Not Be Enough

AUDITORS ARE NOT FRAUD INVESTIGATORS

By Colum Bancroft

On May 22, 2011, Deloitte Touche Tohmatsu CPA Ltd announced its resignation as the auditor of Longtop Financial Technologies Limited, a software developer headquartered in China and listed on the New York Stock Exchange. The trigger for Deloitte's resignation was their discovery that certain statements and confirmations received from one of Longtop's banks were false. Longtop is one of several Chinese overseas listed companies under investigation for fraud, and these various scandals have resulted in falling stock prices, delistings, and lawsuits.

For years, Longtop misled its bankers, clients, investors, and auditors. Although many were quick to blame the auditors for missing the warning signs, investors need to understand that auditors are not as experienced as fraud investigators in being able to spot and question potential red flags. A more detailed examination of the Longtop scandal shows some of the limitations of traditional audit practice for fraud prevention.

Deloitte's resignation letter released in the public domain states that, during a round of bank confirmations on May 17, 2011, officials from Longtop appeared at the bank and prevented the auditors from leaving until they surrendered the bank confirmation documentation and their working papers. Three days later, the company's chairman called the auditor and confessed that "there was fake revenue in the past so there was fake cash recorded on the books [sic]." He also admitted that "senior management" was responsible for the fraud.

Fraud is not intended to be easy to detect, and schemes committed by management are particularly difficult to uncover. Senior executives are in a position to devise sophisticated arrangements to conceal their wrongdoing by forgery of supporting documents, deliberate failure to record certain transactions, collusion to compromise and override existing internal controls, or intentional misrepresentations to auditors.

Taking Longtop as an example, and how the fraud was perpetrated, a look at reported staff numbers shows that Longtop's sales per staff ratio between 2008 and 2010 remained stable at around $40,000. Was this a potential red flag? One should question a constant ratio such as this, especially when economies of scale, improvements in work efficiency, and hence increased output per head might be anticipated as a business grows.

A further review of the Longtop staff details reveal that about three quarters of its employees had been sourced from third-party human resources companies in return for monthly service fees. Longtop claimed that an un-related company, called Xiamen Longtop Human Resources Services Company Limited, had been involved in hiring the majority of these individuals.

The similar names of the two companies and the unusual staff arrangement are highly suggestive of fraudulent activity and, in early 2011, research reports certainly speculated that an undisclosed relationship existed between the two. Without access to the company's books and records, one can only speculate about the details of the fraud scheme employed by Longtop's management. Two possibilities are that Xiamen Longtop overstated the staff numbers in order to support its own inflated revenue figures, or it may have understated the staff costs in order to boost the apparent net margin of Longtop.

The industry recognizes that revenue is often considered susceptible to manipulation, so were the red flags described above missed or not given due attention by the auditors? It is true that extra attention should be paid to the nature and quality of the audit evidence obtained in this area but what are auditors expected to do?

International Standard of Audit (ISA) 240 states that the "primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management." The auditor's role in fraud prevention when conducting an audit is to obtain "reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error."

To obtain reasonable assurance, auditors are required to maintain "professional skepticism" throughout the engagement. This is a fairly abstract, subjective term, and the degree to which professional skepticism

should be applied depends on various factors, including auditors' experience in relation to the integrity of a company's leadership and their knowledge and experience of the industry.

So audit work may include a combination of compliance (controls) and substantive (transactional) testing. One would also expect auditors to carry out analytical procedures in order to gather more evidence and provide further audit assurance and comfort, especially if "professional skepticism" led them to have concern. Such procedures may include studying the relationship between reported sales revenue and various related parameters – including, among others, purchases and direct expenses, sales outlets, and number of staff – in order to reveal any unusual or undisclosed relationships and seek explanations for the apparent anomalies.

However, auditors are not specifically required to conduct an in-depth fraud risk assessment as part of their audit process. The Audit Committee should consider appointing independent risk consultants to conduct such an exercise, which would assist the external auditors during the initial planning stage of their work when they decide upon the specific nature and scope of audit tests to be followed.

In the absence of an independent fraud risk assessment, auditors may incorrectly perceive a relatively low fraud risk, and claim justification for accepting the information provided by management as sufficient audit evidence, on the basis that ISA 240 also states that "unless the auditor has reason to believe the contrary, the auditor may accept records and documents as genuine."

This may present management with an opportunity to deceive auditors. For example, if senior executives establish vendor companies to record purchases that can be matched against fictitious sales, auditors may request from the company the addresses of such vendors in order to send out confirmation letters. Trusting in the "good faith" of management, the auditors might not have considered it necessary to review further or verify the mailing details, meaning that senior executives or people connected with them could simply receive letters from the auditors and reply with false information.

Back to Longtop, Deloitte may have considered the possibility of Xiamen Longtop being related to Longtop, but the auditors' knowledge of a conflict of interest often depends on information made available to them by management and those charged with governance. They are not trained to conduct detailed background investigations to ascertain whether management, or people connected with management, may be behind particular companies; nor are they required to do so. IAS 550 "Related Parties" requires auditors to obtain written representations from management and, where appropriate, those charged with governance, to confirm that all the related party relationships of which they are aware have been disclosed to the auditor.

The recent accounting scandals in China should serve as a collective wake-up call for auditors to strengthen oversight and implement more rigorous procedures in certain areas. Disclosure of poor corporate governance and malfeasance are definitely a blow to a company's reputation, affecting its ability to raise funds from investors or secure bank financing. Creditors may recall debts and borrowing costs increase when stakeholders lose confidence in a company. Auditors are likely to resign when they believe that their previous trust in senior management was misplaced and that the engagement may have a negative impact on their reputation. The results could be disastrous: Longtop was delisted by NYSE two months after Deloitte's resignation.

In order to effectively prevent and detect fraud before it becomes front page news, in addition to the external audit, management and Audit Committees should arrange for an independent fraud risk assessment and the implementation of a comprehensive fraud prevention program.

Colum Bancroft is a managing director based in Hong Kong and leads Kroll's Financial Investigations practice across Greater China. Colum has extensive experience assisting clients on local and multijurisdictional issues in areas such as asset tracing and recovery; family, partnership, shareholder, and other business disputes; insider dealing and share price manipulation; money laundering; and fraud and misappropriation of assets.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **PROFESSIONAL SERVICES**

As in the past, professional services companies had relatively good fraud numbers compared to other industries. The number of companies hit by fraud dropped markedly, and was the second lowest of any sector. Moreover, the industry had the fewest businesses hit by theft of physical assets (15%), procurement fraud (12%), or financial mismanagement (6%). Difficulties remain, however. Even with the smaller number hurt by fraud, the industry's average loss of revenue (2.0%) is only slightly less than the survey norm (2.1%). Moreover, a higher number of companies this year are experiencing an increase in exposure. The two areas requiring most attention are information theft and IP theft. For both—despite a noticeable drop in the prevalence of information theft—professional services companies performed about the same as the survey average. Moreover, they were more likely to feel highly or moderately vulnerable in these areas than other businesses, and IT complexity was the biggest—and a growing—cause of increased fraud exposure in the last 12 months.

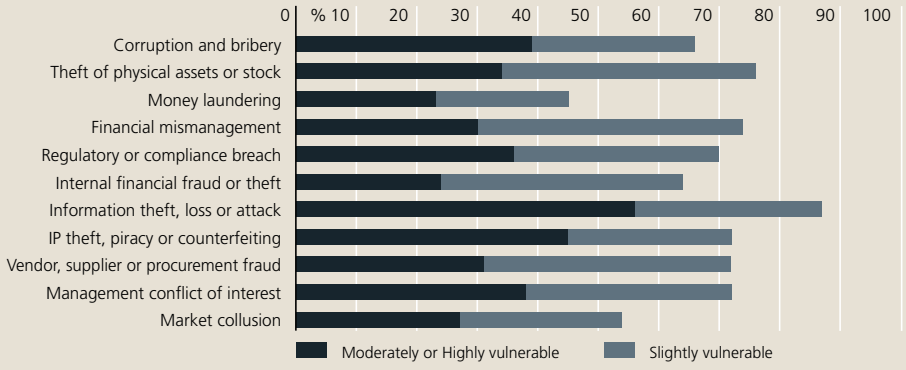
Prevalence: Average percentage of revenue lost to fraud: 2.0%

Prevalence: Companies affected by fraud: 67%

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud: Information theft, loss or attack (23%) • Theft of physical assets or stock (15%)

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: IT complexity (37%)



INDIA OVERVIEW

	2010-2011*
Prevalence: Companies affected by fraud	84%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Corruption and bribery (31%) Information theft, loss, or attack (27%) Internal financial fraud or theft (23%) Theft of physical assets or stock (23%) Vendor, supplier or procurement fraud (22%) Financial mismanagement (22%) Management conflict of interest (19%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (78%) Vendor, supplier or procurement fraud (59%) Information theft, loss, or attack (58%)
Increase in Exposure: Companies where exposure to fraud has increased	85%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	High staff turnover (41%)
Loss: Average percentage of revenue lost to fraud	2.2%

*Insufficient respondents in 2010 to provide comparative data.

India has a number of significant fraud problems. Its prevalence there (84%) is among the highest in the survey, behind Africa but in line with China.

Respondents in India said that corruption and bribery is the most common fraud type they experienced in the past year. Moreover, 78% indicated that their organization is very or moderately vulnerable to the problem, higher than the overall Asian average of 63%. Despite these concerns, only 25% of respondents in India say their organization is well prepared to comply with anti-corruption legislation.

Corruption is only part of the problem. India has a higher prevalence than the overall average for eight of the 11 frauds covered in the survey. In particular, India has one of the highest rates of information theft, loss, or attack (27%), which is of particular relevance in a country that relies so much on its IT sector for growth and development.

Fraud concerns are on the rise. The number of companies in India with growing exposure to fraud (85%) is the highest for any country or region. The country also has one of the largest proportions of respondents (41%) saying that high staff turnover is driving this growth, and the highest percentage saying the same about increased collaboration between firms (27%).

Companies in India do not appear to be investing in the right anti-fraud measures. Results indicate that less than 50% of respondents in India invest in employee background screening, partner or third party due diligence, and risk management systems – a surprising finding given that 59% of those that suffered from fraud and knew the culprit said it was an inside job. Measures such as third party due diligence, effective and well understood whistle blower systems, and well-tested internal risk management systems would help companies in India reduce losses to fraud and corruption.

Corruption and the Indian Infrastructure Boom

By Ramon Ghosh

Any visitor to India will see an array of rickshaws, carts, motorcycles, cars, buses, and livestock squeezed on to potholed, badly maintained roads. While this may provide a good photo opportunity for passing tourists, it is a continuing source of frustration to residents and has severe consequences for the Indian economy. Every train derailment, bridge collapse, or gridlocked highway means a loss for the country's finances.

The government has initiated a number of projects as part of its drive to improve India's infrastructure. These include plans to spend more than $1 trillion over the next 10 years to build new roads, bridges, and ports, as well as modernize India's aged railway lines. Despite these promising plans, these initiatives have been met with many obstacles along the way. For example, the Golden Quadrilateral – a $13 billion highway project to connect India's four metro cities (Mumbai, Chennai, Kolkata, and Delhi) due to be completed this year – was at the center of corruption allegations.

This comes as little surprise. Bribery, together with poor infrastructure, have long been significant problems for the country. Corruption in India has also recently come to the forefront as a high profile issue. Activist Anna Hazare staged a series of hunger strikes in an attempt to force the government to accept proposals for an independent anti-corruption ombudsman laid out in a version of the Lokpal Bill advocated by activists. While the government has engaged on the issue, it remains to be seen whether the anti-corruption movement's demands will ultimately be met. If they are, there will be increased transparency for all government entities, and this will affect how contracts are awarded and serviced in the infrastructure sector.

This year's Global Fraud Survey shows how pervasive the problem of corruption is in India: 78% of respondents in India say that their organizations are highly or moderately vulnerable to corruption and bribery, compared with 47% of global respondents and 63% of those in Asia. Kroll has witnessed first-hand how this affects India's infrastructure industry. The frequent lack of managerial accountability in the sector can create an environment conducive to cash kickbacks between contractors and sub-contractors, who are frequently engaged in regional areas. Pressure can also occur to make facilitation payments to local landowners – if payments are not made, then communities can act to stop construction taking place and works can be disrupted and delayed. In states such as Jharkhand, for example, it is common to encounter physical security threats to people and property when acquiring land and requests for payment for protection against the disruption of operations by Maoist guerillas.

The growing number of anti-corruption laws with extraterritorial reach – such as the United States Foreign Corrupt Practices Act (FCPA) and the UK's recently enacted Bribery Act (UKBA) – means that the regulatory risks involved with corruption are not just restricted to overseas investors: many Indian entities will also be subject to the multi-jurisdictional obligations of these pieces of legislation. In particular, the UKBA expands the scope of regulatory risk into the area of facilitation payments. This has particular relevance for India's infrastructure sector, where land acquisition has long been a compliance grey area. Two examples that Kroll has seen of how companies could fall foul of

the extraterritorial UKBA prohibition on making facilitation payments are (i) payments being made to village heads and local landlords who may, in turn, use their influence to help acquire land from farmers at below market price and (ii) making payments to land owners when they demand a premium on the market value of their property to ensure ownership. Kroll has seen instances where farmers and local land owners have been paid up to 50% of the value of the land in cash or "black money" as an incentive for the seller so that it does not have to be disclosed as income. The exchange of black money, though, would be in clear contravention of the UKBA, under which ignorance is not a valid legal defense.

While chasing the potentially lucrative returns available in the Indian infrastructure sector, businesses must have adequate procedures in place to prevent corruption, including facilitation payments. At the very least, companies should carry out a thorough audit of their internal procedures to make sure that they comply with the FCPA and the UKBA, and that their employees are not adopting dubious local practices. Putting in place an effective whistle-blowing system can also help, but in order to get proper buy-in from employees it needs endorsement from the top of the company and the assurance of complete confidentiality for those who use it.

On top of such practical measures, it is vital that foreign companies fully understand the culture of business in India. The use of facilitation payments is widespread across many sectors, particularly those that involve negotiations or approvals from government agencies. Investors unaware of such practices might incur serious legal and reputational harm.

The events surrounding the Lokpal Bill show the increasing appetite for change in India. A culture of corporate compliance is now likely to become more important when doing business in the country. Companies must, therefore, be aware of the need for forward thinking when reviewing their existing systems. In the infrastructure sector, the potential returns are vast but these must be realized in an ethical way and always with an eye to compliance.

Ramon Ghosh is a senior director with Kroll's operations in India. Ramon is a qualified solicitor (England & Wales) and spent a number of years working as a commercial litigation lawyer for international law firms. Ramon has been involved in in-depth investigations, evidential analysis, witness proofing and mitigation strategy discussions on a number of cases.

EUROPE OVERVIEW

European companies continue to do well relative to the rest of the world when it comes to fraud. They have a lower than average incidence of every fraud covered in the survey except market collusion (9%), which is only slightly above the global norm.

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	71%	83%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (23%) Management conflict of interest (19%) Information theft, loss, or attack (18%) Internal financial fraud (16%) Vendor, supplier or procurement fraud (14%)	Theft of physical assets or stock (23%) Information theft, loss, or attack (19%) Vendor, supplier or procurement fraud (14%) Management conflict of interest (13%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Information theft, loss, or attack (47%) Theft of physical assets or stock (41%) Management conflict of interest (39%)	Information theft, loss, or attack (37%) Theft of physical assets or stock (32%) Regulatory or compliance breach (28%)
Increase in Exposure: Companies where exposure to fraud has increased	74%	73%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (33%)	IT complexity (29%)
Loss: Average percentage of revenue lost to fraud	2.0%	Not available

A comparison with last year however yields a picture of a growing fraud problem. Unlike much of the rest of the world, compared to last year the region saw no decline in the prevalence of the theft of physical assets (23%), and only a small drop in information theft (from 19% to 18%). Moreover, out of the 11 fraud types covered in the survey, the incidence of six has significantly increased over the last year and moderate increases were seen with three. Management conflict of interest (19% up from 13%), corruption (14% up from 8%), and financial mismanagement (19% up from 12%) in particular saw striking growth. Furthermore, in last year's survey 47% of European companies said that they had suffered no financial losses from fraud; this year that figure dropped to 23%.

Meanwhile, anti-fraud measures are not being implemented proportionate to the growing prevalence. European companies are currently less likely than average to deploy every such strategy covered in the survey. In particular, employee background checks (34%) are much less widespread than the global average (47%), despite respondents indicating that, when fraud occurred and the culprit was known, it was frequently committed by a junior employee (25%) or senior manager (23%).

The Biggest Threat to Financial Institutions: It Comes from Within

By Richard Abbey

The statistics from the 2011 Global Fraud Survey show that, once again, financial institutions are a prime target. The greatest threats which they face are often thought to come from outside the institution and involve crimes such as data theft, credit card fraud, identity theft, bank fraud, and attempts at fraudulent transfers: A significant amount is lost to these frauds so it is no surprise that financial institutions spend substantial amounts of money on dedicated teams and sophisticated technology to monitor and prevent such avoidable losses.

However, alongside these external threats is an even bigger risk: greed, in the shape of the eternal yearning inside these companies for increased profits.

History has shown that, in a large number of cases, employees themselves have caused the greatest damage to individual financial institutions. Substantial losses have been incurred – and in several instances entire companies have collapsed – as a result of the actions of a group of individuals, or even a single person, within the business.

Since the ongoing financial turmoil first began over four years ago, Kroll has been asked to investigate the circumstances surrounding the collapse of major financial institutions in at least four different jurisdictions in Europe and the Middle East. A recurring theme of each investigation has been that individuals in powerful positions at the companies in question were, or at least should have been, aware of activities that were exposing the institution to significant risk. Policies and procedures designed to safeguard the organization were either not followed or "creative" transaction structures were used to bypass them.

Senior executives typically allowed such activity to go unchecked for one of two reasons, depending on circumstances: when times were good, the business generated significant profits; as the credit squeeze took effect and the economy turned, past excesses needed to be covered up. Either way, the behavior demonstrated that controls work only if they are actively implemented, and even the most stringent ones will be ineffective when collusion is used to work around them.

The auditors, too, were often not without blame. In several of these investigations, serious questions arose about their role in identifying the issues that ultimately contributed to the collapse of the financial institution in question. In many instances the auditors failed to look in the right places: the audit procedures undertaken were too standardized or they did not consider the fundamental substance of what was happening over its form. On other occasions, the relationship between auditor and client was unhealthily close. This was often true in emerging markets where only a small number of qualified professionals were available to deal with a large number of high growth businesses.

What can a financial institution do to protect itself? First, it should ensure that it implements a rigorous risk management policy

and internal reporting structures which are actively monitored and tested for adherence. Second, it should make certain that the board and any internal risk committees adequately understand how and where the institution is making its profits, the risks associated with those transactions, and how they are being managed. Finally, the board should see to it that independent risk assessments are routinely carried out on the company's most profitable divisions to ensure that the controls in place are adequate and that the transactions it is undertaking make sense in terms of the profits derived and true potential exposure. Such work is not the stuff of normal audits, and should be conducted by expert financial investigation firms as opposed to a company's usual auditors.

Richard Abbey is head of Kroll's London financial investigations practice. He has 16 years' experience in forensic and financial investigations. He has managed complex international frauds, multi-jurisdiction asset-tracing and large accounting investigations, including a number of alleged breaches of the Foreign Corrupt Practices Act. Richard's investigations have covered many industries, and he has appeared as an expert witness in both civil and criminal matters. He has also commented on white collar crime for numerous media outlets.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — FINANCIAL SERVICES

Despite some notable progress against information theft and theft of physical assets, this was another difficult fraud year for the financial services industry. It had the highest rate of loss of any sector (2.7% of revenue) and the highest prevalence of information theft (29%), internal financial fraud (29%), regulatory and compliance breaches (19%), and money laundering (10%). It is therefore understandable that respondents from this sector are more likely than average to feel very or moderately vulnerable to every fraud covered in the survey, except IP theft, where they feel only slightly less vulnerable than average. On the positive side, financial services companies are more active than most in addressing fraud. They are more likely on average to invest in the coming year in every anti-fraud strategy covered in the survey, and are the most frequent investors in six out of 10: risk systems (35%), IP protection (34%), management controls (34%), financial security measures (33%), employee background screening (30%), and asset security measures (29%).

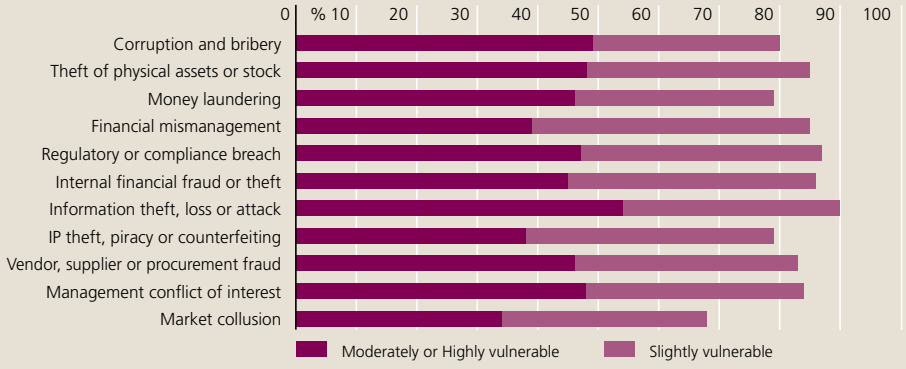
Loss: Average percentage of revenue lost to fraud: 2.7%

Prevalence: Companies affected by fraud: 80%

Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud:
Information theft, loss or attack (29%) • Internal financial fraud or theft (29%) • Financial mismanagement (18%) Management conflict of interest (24%) • Theft of physical assets or stock (23%) • Corruption and bribery (22%) Vendor, supplier or procurement fraud (21%) Regulatory or compliance breach (19%)

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: IT complexity (43%)



Corporate Investigations in Strict Privacy Regimes

The Case of Italy

By Marianna Vintiadis

Over the past couple of decades, European countries have adopted legislation which has increasingly strict privacy-related rules and regulations. Italy's regime in this regard is complex and, in many respects, draconian.

What often worries corporate executives the most about Italy's privacy laws is the attribution of criminal liability to company directors when the rules are breached. In one widely publicized case, three Google directors were convicted in 2010 of breach of privacy. The New York Times reported on February 24 2010, "In Milan, Judge Oscar Magi sentenced the Google executives in absentia to six-month suspended sentences for violation of privacy. Prosecutors said Google did not act fast enough to remove from the site a widely viewed video posted in 2006 showing a group of teenage boys harassing an autistic boy." Those convicted included Google's Privacy Director and the former Chairman of Google in Italy who, at the time of the conviction, was Senior Vice-President and Chief Legal Officer for the company.

If privacy law is a worry at the best of times, a case of fraud or other white collar crime requiring an internal investigation is likely to produce shudders in boardrooms. Such a reaction can result in a propensity to turn a blind eye or in the temptation to settle the problem through a termination of employment, without a full investigation of the facts which may in itself create further liability for the company. When combined with the fear of upsetting the country's powerful labor unions or breaching provisions of the law protecting employees, the Statuto dei Lavoratori, the result can be paralysis.

Acting without a proper investigation of the facts, however, can lead to mistakes and can mean that a problem is only partially solved. Complex corporate frauds can require the participation of many employees in different departments. The failure to carry out a thorough investigation of all facts and persons involved, can lead to the dismissal of a single person which may leave the illicit activity unimpeded and allow its revival after the dust has settled. Moreover, terminating employment without carrying out a thorough investigation can often mean foregoing damage recovery and may even prove a very costly option in the absence of evidence. An even bleaker prospect is that an Italian court can order a company to reinstate unlawfully dismissed employees.

Strict privacy regimes should not, however, be an impediment to internal investigations which are in some cases compulsory, for example, in certain whistle-blowing cases – the employer is required to carry out an investigation. It is therefore important for employers to be aware that they have tools at their disposal that do not violate Italy's tough privacy laws when trying to detect and collect evidence of internal fraud.

The first thing to understand is that investigations do not have to invade personal privacy. Many involve desktop analysis of publicly available information. Take the scenario of a manager having a conflict of interest because he, or a member of his family, owns a company supplier. In such cases, an analysis of corporate records and information on immediate relatives available through the general registry may be sufficient to obtain the required proof of conflict of interest.

Another important tool is the use of computer forensics to recover and analyze data present on the computers of employees. Accurate information on the subject for those outside the legal profession is hard to come by and relatively few Italian law firms have this expertise in-house. Many executives believe that the accessing of an employee's corporate email account is always a violation of "private correspondence." However, the Italian Supreme Court has, in fact, made a clear distinction between open and closed correspondence, placing corporate email in the former category which indicates that, in certain circumstances an employer may be entitled to access an employee's corporate email account providing, of course, such access is in accordance with applicable laws and regulations and with the company's own policies.

Many factors, including a company's internal policies and regulations play a part in shaping what can and cannot be done in each case. As the rules are so complex and turn on the facts of each particular case, legal advice should be sought in each case before deciding on the recovery process, the investigation plan, and the relevant exclusions in order to ensure that the actions of investigators and technicians will not undermine the validity of the evidence gathered.

When the rules are followed, however, computer forensics can constitute an extremely powerful instrument. In Italy, where Internet usage still lags behind the European average and many families do not own a computer, Kroll has found that unscrupulous employees will often conduct their business using company computers and even corporate email accounts. Moreover, many individuals labor under the false assumption described above that Italian law prevents the employer from accessing their devices no matter what the circumstances. Many believe that the rules prohibiting Italian employers from monitoring employee activity mean that no type of enquiry or investigation is allowed at all.

As a result, in many cases, cheating employees pay very little attention to covering their tracks. Often, therefore, the evidence recovered through computer forensics is very strong and sufficient either to make a case or to extend investigators' understanding of the so-called circle of knowledge. This latter outcome can be as important as a smoking gun, because *prima facie* evidence of involvement in the criminal activity under investigation can be sufficient to extend the scope of the investigation itself.

Another helpful tool in investigations is surveillance. Once again, this very widely used instrument in Italian investigations is often misunderstood. There is a general belief that it represents an automatic breach of privacy for those being watched. This is not necessarily correct: surveillance is very highly regulated and subject to significant limitations, but in certain circumstances its use is legal and evidence collected through its deployment can in some cases be submitted in court.

These are not the only investigative tools and techniques available to employers. For example, many internal investigations also rely heavily on forensic accounting and interviews. Typically, an enquiry will require the combination of a number of different tools. It is therefore important to have the right legal advice, proper investigative backup, and the unions on board before deciding how to tackle an internal problem. The message, though, is clear: strict privacy laws need not obstruct the carrying out of internal investigations.

Marianna Vintiadis is Kroll's country manager for Italy and Greece. A trained economist with experience in policy making and analysis, she works on business intelligence and complex investigations in these countries. Her areas of expertise include market entry, shipping, piercing the corporate veil, and internet investigations.

MIDDLE EAST OVERVIEW

While the number of companies that suffered from fraud last year fell to 68% from 86% the year before, it is still a concern in the Middle East.

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	68%	86%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Information theft, loss, or attack (26%) Vendor, supplier or procurement fraud (25%) Management conflict of interest (23%) Corruption and bribery (21%) Internal financial fraud or theft (19%)	Information theft, loss, or attack (30%) Theft of physical assets or stock (30%) Internal financial fraud or theft (21%) Financial mismanagement (19%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (62%) Information theft, loss, or attack (54%) Management conflict of interest (48%)	Information theft, loss, or attack (49%) Regulatory or compliance breach (47%) Financial mismanagement (47%)
Increase in Exposure: Companies where exposure to fraud has increased	77%	70%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	IT complexity (33%)	IT complexity (35%) Entry into new, riskier markets (35%)
Loss: Average percentage of revenue lost to fraud	2.6%	Not available

This year, the region has seen the number of respondents facing increased exposure to fraud grow to 77% from 70% last year. More worrying, there has been substantial growth in several specific types of fraud: vendor, supplier, or procurement fraud hit 25%, up from 9% last year; corruption and bribery affected 21% of companies, also up from 9%; and management conflict of interest was present in 23%, nearly double last year's 12%.

As a result, concern over these frauds is growing markedly: 42% of respondents rank themselves as at least moderately vulnerable to procurement fraud (up from 26% last year) and 48% to management conflict of interest (up from 40%).

Concern about corruption and bribery is even greater: 62% say their organizations are highly or moderately vulnerable (up from 30% last year) and 37% admit that they are not prepared to comply with anti-corruption regulations – the highest figure for any region.

Despite such worries, companies are undermining their own anti-fraud efforts: 32% of respondents in the Middle East said that weaker internal controls are increasing their exposure to fraud, up from 14% last year and much higher than this year's survey average of 22%. If businesses are to face the growing exposure to fraud, they must strengthen such controls.

Corruption and Vendor Fraud in the Gulf

PRACTICAL ADVICE

By Yaser Dajani

The last few years have shown that the Gulf economies are not insulated from global trends. In particular, the financial crisis and its fallout exposed fraud in the region like never before, showing it to be remarkably similar to fraud elsewhere. With several key financial hubs in the region exhibiting limited signs of recovery, a number of markets – including Saudi Arabia, Kuwait, Qatar, and the United Arab Emirates – have seen a surge of activity. What do companies based in the region and those seeking to enter it need to do to mitigate their exposure to fraud?

According to the Global Fraud Survey, corruption and vendor or procurement fraud are the fastest growing types of fraudulent activity observed in the region. The latter affected 25% of respondents last year, up from 9% in 2010, while corruption hit 21%, also up from 9%. Whether these figures reflect a true increase or a greater recognition of these frauds by executives, companies need to deal with them. The following specific examples will provide some insight.

Government contracts in the Saudi construction market

Saudi Arabia has a booming construction market with an annual budget exceeding $80 billion earmarked by the Saudi government. The Kingdom is using this money to develop six economic cities, 27 airports, and various train networks and highways. The Kingdom is also pursuing major development projects in key areas including Riyadh, Jeddah, and the oil-rich Eastern Province. The majority of large contracts are awarded by the Saudi government-related enterprises. To penetrate this market, regional and international construction companies are forming joint ventures or partnerships with local Saudi businesses, most of which are family-owned.

The Saudi construction market is complex and operating under an evolving regulatory framework. Anti-bribery laws exist and government officials are prohibited from assuming active positions in companies, but the rules are not always well defined. This lack of clarity can leave companies exposed to regulatory risk. Although rare, corruption investigations in the country do take place. In 2010, the government established a Saudi Commission to investigate the infrastructure's inability to withstand a flood which resulted in a major collapse in the Jeddah Governorate.

In looking for the right business partner in this environment, one should focus on:

- **The management of family-owned businesses:** In Saudi Arabia, control of companies is typically "generational," with management passed on from fathers to sons. Understanding the management of recent transition and whether or not corporate controls have been introduced are crucial; a robust governance system provides comfort to potential partners regarding a company's code of conduct.
- **The company's classification by Saudi ministries:** Most businesses in the industry have a grade between one, the highest, and four, the lowest, which regulates the scope and value of the projects on which local companies permitted to work. This official classification can serve as an important indicator of a company's strengths and

weaknesses in the market, as well as a tool to gauge the extent of potential exposure to corrupt practices.

» **The place of company principals within the Kingdom's elite:** In some cases, contracts are awarded to companies based not only on the owning family's position in the Saudi social and political fabric but also on the proximity of shareholders to the ruling family, the Al Saud. Knowledge of how relationships are structured is often the key to understanding how businesses operate in the country. One of the key complications of doing business in Saudi Arabia is that this commercial strength can potentially carry FCPA/UK Bribery Act risk. We can help distinguish between strong relationships without such risk, and strong relationships with risk.

» **Reasons for previous success:** How a company has won past tenders, especially large contracts may reveal important information. If a potential joint venture or partnership moves forward, it is important to exercise joint control over the bidding process and financial expenditures.

In looking into these areas, companies should avoid over-reliance on the public record, which is undependable. In Saudi Arabia it is typically people, not documents, which hold information.

Distribution agents in the Gulf

Vendor or procurement fraud in the Gulf region often involves local agents, who commonly represent companies in the consumer goods, information technology, retail, insurance, and professional services sector. In most cases, agents divert business or products away from the company they are representing by setting up parallel corporate entities, and in other cases agents become involved in counterfeit activities. This helps explain why the reported prevalence of management conflict of interest in the region has also increased from affecting 12% of companies in 2010 to 23% in 2011. This particular conflict is amongst the most pernicious, damaging and widespread.

When appointing an agent in the Gulf, companies should consider several factors:

» **Relationships with third parties:** Companies in the consumer goods sector should examine their local partners' distribution channels and ensure that they maintain effective access to key markets. Local agents often use multiple re-sellers thereby obscuring the supply chain and raising the potential for "diversion risk" to restricted markets.

» **Related-party transactions:** Review and ensure full disclosure of related-party transactions to understand their objectives and relevance. Some sister companies provide each other with services—which can be valuable at times—however in some cases there is over-invoicing for no actual services rendered.

» **Offshore Incorporation:** Local agents often establish representation in free zone jurisdictions, which are not subject to international standards of disclosure or regulatory oversight, thereby hindering transparency. Agents should disclose their corporate information and constituents before being selected.

» **Multiple businesses:** Agents frequently control or own multiple businesses but do not disclose their existence or nature. These undisclosed relationships carry particular ramifications if such companies interact with disreputable organizations or sanctioned entities, such as trading with Iran in prohibited items such as dual-use equipment. Regulatory action against the agent will have implications on the parent company and might disrupt the provision of royalties and other payments.

Despite increases in certain types of fraud in the Middle East, including bribery and procurement fraud, the data shows that some companies have successfully reduced their fraud incidence in the Gulf. Knowledge and understanding of local red flags can help companies go a long way towards protecting themselves.

Yaser Dajani is an associate managing director with Kroll's Middle East practice based in Dubai. Yaser focuses on complex business intelligence and due diligence investigations. His core areas of expertise include market entry, corruption risk assessments, anti-counterfeit support and litigation support and asset recoveries. He works across a wide range of sectors and geographies in the MENA region.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **CONSTRUCTION, ENGINEERING & INFRASTRUCTURE**

Despite another noticeable improvement in overall incidence this year, the construction industry still has a problem with several of its traditional fraud issues. Theft of physical assets increased, affecting 32% of companies, the third highest industry figure. Corruption—a particular temptation for still-struggling companies in the developed world that may need government contracts in order to prosper—hurt 24% of construction businesses, the second highest industry level. Finally, the sector has an above-average incidence of market collusion (11%). Unlike last year, this year's survey indicates that construction companies are less focused on fraud prevention. Construction firms are less likely to invest in eight of the 10 anti-fraud strategies covered in the survey. More worrying, this sector is least likely to put extra money into employee background checks, even though high staff turnover remains the biggest driver of increased fraud exposure.

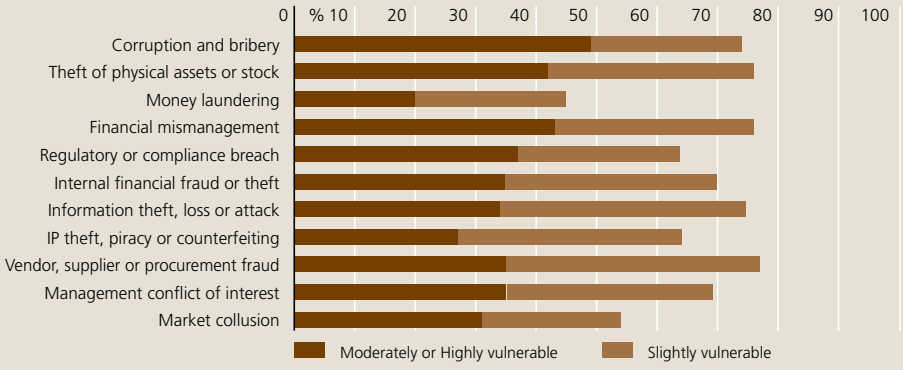
Loss: Companies affected by fraud: 1.9%

Prevalence: Companies affected by fraud: 69%

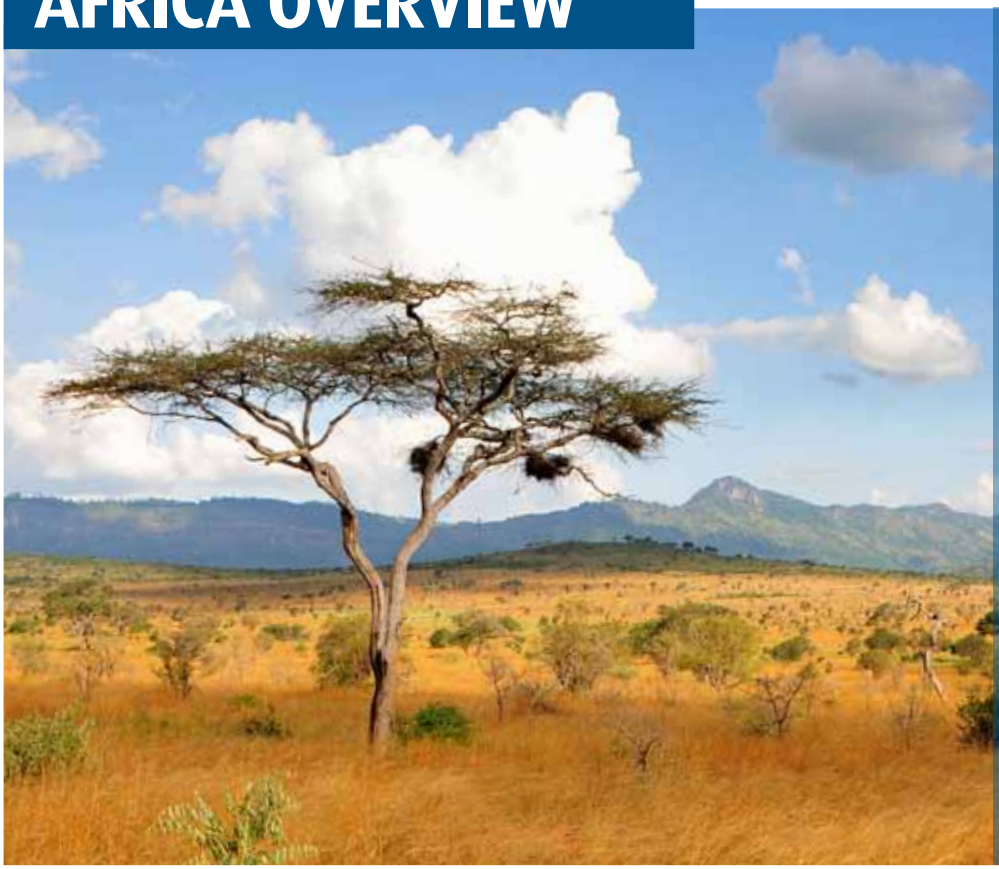
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud
Theft of physical assets or stock (32%) • Corruption and bribery (24%)
Management conflict of interest (21%) • Vendor, supplier or procurement fraud (19%)
Financial mismanagement (17%) • Information theft, loss or attack (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 (28%)



AFRICA OVERVIEW



Africa continues to struggle with one of the worst fraud environments in the world. It has the highest overall incidence (85%) of any region. Although information theft, loss, or attack saw a marked decline – from 41% last year to 22% this year – fraudsters seem only to have changed their methods rather than to have been thwarted. For five of the 11 frauds tracked in the survey, Africa had the highest incidence of any region: theft of physical assets (38%); corruption and bribery (37%); internal financial fraud (33%); financial mismanagement (32%); and money laundering (13%).

	2011-2010	2010-2009
Prevalence: Companies affected by fraud	85%	87%
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud	Theft of physical assets or stock (38%) Corruption and bribery (37%) Internal financial fraud or theft (33%) Financial mismanagement (32%) Vendor, supplier or procurement fraud (31%) Management conflict of interest (27%) Information theft, loss, or attack (22%) Market collusion (14%)	Information theft, loss, or attack (41%) Theft of physical assets or stock (41%) Management conflict of interest (39%) Financial mismanagement (35%) Internal financial fraud or theft (30%) Vendor, supplier or procurement fraud (26%) Regulatory or compliance fraud (20%) Corruption and bribery (17%) Market collusion (15%)
Areas of Vulnerability: Percentage of firms considering themselves moderately or highly vulnerable	Corruption and bribery (78%) Theft of physical assets or stock (68%) Internal financial fraud (67%)	Vendor, supplier or procurement fraud (59%) Information theft, loss, or attack (58%) Management conflict of interest (54%)
Increase in Exposure: Companies where exposure to fraud has increased	84%	70%
Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected	Weaker internal controls (35%)	IT complexity (39%)
Loss: Average percentage of revenue lost to fraud	3.1%	Not available

Corruption is a particular problem: 37% of African companies said that they were affected in the last year, more than twice the figure in the 2010 survey (17%). More alarming still, 78% of respondents said their company is highly or moderately vulnerable to this fraud, up from 44% last year.

Fraud continues to deter companies from working in Africa. This year, it remains the region where the experience or perception of fraud has dissuaded the most companies from operating (15% of global respondents). Of those dissuaded, 69% cited corruption as one of the leading causes for the decision, although theft of physical assets (26%) and information theft (24%) were also common factors.

As ever, companies in Africa are trying to stem the tide of fraud. Most anti-fraud strategies are already more widespread there than elsewhere, and more Africa-based companies plan to invest further in several areas – such as staff training, employee background screening, and third party due diligence – compared to the global average, At the same time, however, over a third of companies are also seeing weaker internal controls due to cost-cutting, which will negate some of the anti-fraud investment.

AFRICA
Are We There Yet?

By Melvin Glapion and Béchir Mana

For years, forecasters have been proclaiming that Africa's hour has arrived. Several unprecedented trends are making that hope especially strong at the dawn of this new decade. Africa is among the fastest developing regions in the world, with continental GDP growth expected to reach 5.5 percent in 2011 and 5.9 percent in 2012. Moreover, the region's countries are not just supplying commodities to China and the West. A virtuous circle is expanding the African middle class and boosting domestic demand: higher education is becoming much more common, leading to numerous well-paid jobs in booming sectors, which are in turn raising standards of living, leading to the opportunity to pay for better education.

Unlike struggling developed economies, emerging markets such as those in Africa have shown a capacity for continued growth. Business leaders working there may have thought that they faced high levels of risk before 2008, but after the financial crisis, African investments can seem less risky than those in many developed countries. So, has Africa's time come? Are we there yet?

Based on this year's Global Fraud Survey, one might be inclined, erroneously, to think that the news is grim for those pondering African investment opportunities. The results show, for example, that average fraud losses on the continent are higher than in any other region and that fraud worries are a bigger impediment to attracting companies to Africa than anywhere else.

One might therefore assume that investment in Africa is on the wane, but this could not be further from the truth. The value of mergers and acquisitions (M&A) deals completed in sub-Saharan Africa for 2011 is expected to top the $44 billion recorded in 2010, which was itself double the 2009 figure. This activity goes well beyond extractive industries: of the 10 largest M&A deals in Africa last year, only four involved that sector. Similarly, the largest deal thus far this year has been the $1.3 billion sale of Cape Town's Victoria and Albert Waterfront Mall. Even private equity is getting into the act, with its sub-Saharan investment growing 60% last year.

Africa is definitely providing new hope for investors. In spite of the varied and sometimes significant risks in Africa, the opportunities cannot be easily overlooked, particularly given the lower price of assets than in North America and Europe. In business, though, the more tantalizing a market seems, the more investors should be cautious. Foreign investors are often unfamiliar with the potential risks of investing and operating a business in Africa and could lose money because of it.

Current Focus in African Risk Management

Prevent	Detect	Recover
Partner/Target Screening	Financial Controls	External Investigations
Employee Screening	Inventory Management	Internal Investigations
Senior Hire Screening	Physical Security	External Forensics
Risk Assessment	IT Security	Internal Forensics
Risk Management	IT Counter Measures	External Legal
Employee Training/Whistleblower	Audit Committee	Internal Legal

Future Trends in African Risk Management

Over the years, we have found that those investors who successfully manage and mitigate risks in Africa share three key attributes:

1. They understand the nuances: Treating Africa as a monolithic whole obscures local understanding. Consistently successful investors in Africa make rigorous assessments of the nuances of each investment opportunity from a country, regional, and industry perspective. Such an assessment need not be long and arduous, or expensive, in order to give a clear indication of where vulnerabilities may exist. This in turn can help businesses in deciding how to structure, partner, manage, and monitor investments.

One useful approach for gaining a better understanding of the local situation is to apply what we call a M–O–R–T–A–R analysis to the country and market environment of the investment. We have created the concept of MORTAR as a reaction to the 'BRIC opportunities' way of thinking, currently in existence. MORTAR is a risk assessment paradigm used to address a series of possible red flags.

Consideration of an investment's country and sector in the light of each of these issues can provide some guidance on where to focus mitigation efforts. For example, a lack of market and industry data should prompt investors to spend additional time in conducting more "on the ground" human intelligence research, which will likely be more reliable than government statistics; in those countries where corporate governance is wanting, it would be wise to make certain that there is a strong culture of anti-corruption and anti-bribery, as well as rigorous processes to ensure that employees and agents are compliant with local and international law as well as with company policies and procedures; or, in circumstances where there is a weak or absent judiciary, investors need to consider how they might be able to recover in the event of fraud or to use the limited remedies available to them to maximum advantage if necessary.

2. They use the full spectrum of risk mitigation strategies: This year's Global Fraud Survey results indicate that African companies are more likely than Western ones to be planning to invest in due diligence, employee screening, and staff training. This represents a shift – a good one – in the allocation of resources [see figure 1]. Too many businesses in the region focus narrowly on one type of fraud prevention strategy. Experienced investors in Africa have learned that they need to use every risk mitigation strategy available. Moreover, a focus on preventative measures is likely to cost less time and money that might otherwise need to be spent on long and complex recovery efforts after a fraud has occurred.

	Issue	Vulnerability or Challenge
M	Market, industry, and country statistical data is scarce, unreliable, or inconsistent.	■ How do I benchmark levels and degree of fraud? ■ How do I coordinate an industry-led response to fraud? ■ How do I understand the context of the financials of a potential partner or acquisition target?
O	Opaque corporate structures and a lack of clear corporate governance are common.	■ How do I gain an understanding of the ownership structures or financial provenance of partners or acquisition targets? ■ Is the beneficial ownership of a competitor or partner a government entity?
R	Restrictions are placed on access to the public record, especially the press.	■ Have previous controversies around my potential senior-level hire been reported or erased from the public record? ■ How much faith can I put in articles from certain media?
T	Ties to government determine the level of commercial success.	■ How can I be sure my competitor is not unfairly benefitting from a government relationship? ■ How can I be sure that my employees are not running afoul of the law?
A	Absence of a judiciary is compounded by lack of a clear legal framework.	■ What remedies are available to me if I am a victim of a fraud? ■ What level of enforcement support am I likely to receive?
R	Regulatory environment is constantly changing or hard to assess.	■ How does this affect the incentives for my competitors to engage in corrupt practices? ■ How do I ensure my employees are not encouraged to violate the law?

3. They develop a reputation for combating fraud aggressively: Regardless of the specific anti-fraud measures upon which a company relies, long-term success in this battle depends on its reputation among in-country stakeholders for combating fraud.

This local reputation will affect the types of partnerships a business is offered, the integrity of the employees it is likely to attract, and the manner in which customers will engage with it. In Kroll's experience with firms that have successfully addressed fraud risk in Africa while thriving financially, a principled presence in-country, combined with a strong culture of business integrity – supported by the necessary policies, procedures, and structures – is instrumental in not only deterring fraud but also in greatly minimizing the impact should it occur. Contrary to popular belief, fraud prevention is not solely a regulatory function; it is a critical strategic function. Never is this more accurate than when considering an investment in a region with so much potential for reward, and yes, risk.

To manage the complexity of African markets, some business leaders could still be tempted to believe that success depends mostly on political connections, but such shortcuts leave companies greatly exposed to political volatility and reputational risk. On the continent, a compliance-driven approach is the wisest and safest way to take advantage of new opportunities. Such a risk mitigation strategy also brings with it effective accounting, legal and financial management, cultural, and economic insight. Moreover, in Africa, where facts are complex and often hard to ascertain, compliance programs, integrity policies, and above all thorough investigations where necessary are crucial means to strengthen a company's reputation and thereby to secure its business. This is not wasted cost; with the right preventative measures in place, Africa's return on investment becomes unmatched.

The attributes of those investors who are long established in Africa show that lasting business success is possible with the appropriate level of fraud risk mitigation and compliance. In the years ahead, such an approach will allow investors to thrive in this challenging, but increasingly promising, environment.

Melvin Glapion leads Kroll's Business Intelligence practice in London. He has over 16 years of M&A, corporate strategy and financial analysis experience, leading multidisciplinary and multi-jurisdictional teams in conducting cross-border market entry, due diligence and competitive intelligence engagements. Previously he advised on corporate strategy initiatives at KPMG, and has held several other strategy roles within the private sector.

Béchir Mana is a senior managing director. Béchir leads Kroll's operations in France, Africa, Switzerland, Belgium, Netherlands and Luxembourg. He is expert in business intelligence and investigative due diligence, asset-tracing and litigation support, with particular emphasis on French, African and North African assignments. He also advises corporate and government clients on risk, strategy, crisis management, hostile takeovers and corporate affairs. Bechir has managed complex, sensitive policy issues with senior government officials. He has strong expertise in influence, policymaking and lobbying.

Sailing Safe?

For a second successive year, the travel, leisure, and transportation sector registered better fraud figures than those of the other sectors.

It had the lowest prevalence of fraud of any industry overall, although a majority of companies (59%) were still hit at least once. Moreover, these companies saw the lowest level of information theft (12%) and market collusion (4%), as well as a notable decline in the prevalence of several individual frauds, primarily procurement fraud, which dropped from 27% to 17%. Amid the generally positive news, however, are a few worrying trends. The number of companies experiencing an increase in fraud exposure last year has risen from 58% to 71%, and the proportion of companies hit by five of the 11 frauds covered in the survey also rose. In the case of internal financial fraud, this involved a rise from 7% to 16%. Moreover, with success comes the danger of complacency. The industry has the smallest percentage of companies expecting to invest in information security (23%), financial controls (17%), and physical asset security (17%), the last of which was an area with the biggest fraud prevalence in the sector this year.

ECONOMIST INTELLIGENCE UNIT REPORT CARD — **TRAVEL, LEISURE & TRANSPORTATION**

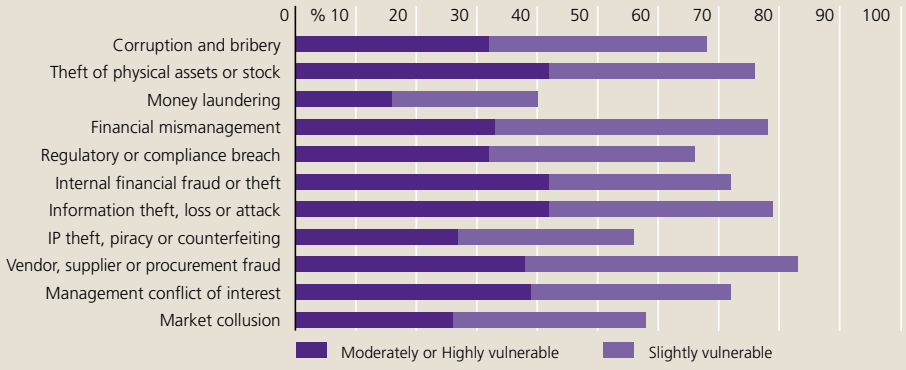
Loss: Average percentage of revenue lost to fraud: 1.9%

Prevalence: Companies affected by fraud: 59%

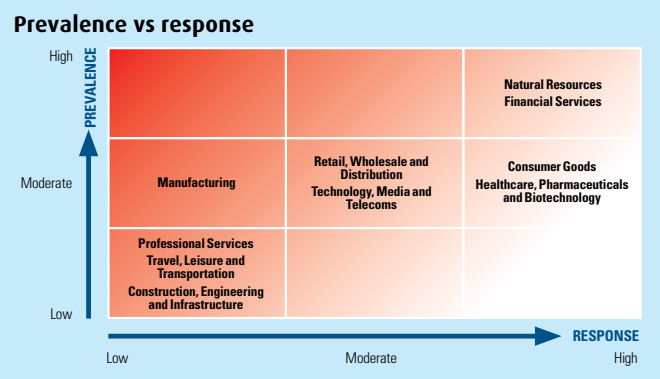
Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud
Theft of physical assets or stock (21%) • Vendor, supplier or procurement fraud (17%)
Internal financial fraud or theft (16%) • Management conflict of interest (16%)

Increase in Exposure: Companies where exposure to fraud has increased: 71%

Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (32%)



Summary of Sector Fraud Profiles



Sector	Prevalence (degree to which sector is exposed to fraud)	Response (degree to which sector has adopted or plans to further invest in fraud countermeasures)	Comment
Natural Resources	High	High	The natural resources sector reported the highest percentage of companies hit by fraud in the last year, with theft of physical assets and corruption cited as the biggest problems. To combat these concerns, companies are heavily investing in a broad range of anti-fraud measures: management and financial controls, information security and physical asset security. The sector recognizes its vulnerability to corruption and plans to increase investment in due diligence, staff training and whistle-blower hotlines over the next 12 months.
Financial Services	High	High	Companies in the financial services sector experienced the highest rate of loss of any sector (2.7% of revenue) and had the highest prevalence of information theft, internal financial fraud, regulatory breaches, and money laundering. Investment in fraud prevention mirror these concerns: the sector is more likely on average to invest in risk systems, IP protection, management controls, financial security measures, employee background screening, and asset security measures. However for a high risk sector these measures should be regularly tested and reviewed.
Manufacturing	Moderate	Low	Manufacturing companies posted the highest incidence of theft of physical assets, procurement fraud, and management conflict of interest of all sectors, with high staff turnover cited as the leading reason for the increase in fraud exposure. Unfortunately, the sector's response to these concerns is poor. Companies plan below average investment in most anti-fraud measures.
Construction, Engineering & Infrastructure	Low	Low	Despite a noticeable drop in the overall prevalence of fraud, construction, engineering & infrastructure companies continue to struggle with theft of physical assets, corruption and procurement fraud. On average, the sector is less focused on fraud prevention compared to other industries. More worrying, this sector is least likely to put extra money into employee background checks, even though high staff turnover remains the biggest driver of increased fraud exposure.
Retail, Wholesale & Distribution	Moderate	Moderate	While the retail, wholesale and distribution sector has experienced a drop in theft of physical assets and information theft, it is seeing a growth in internal financial fraud, market collusion, and even corruption. The sector logs the highest percentage of companies reporting high staff turnover, cost restraints over pay and weakened internal controls as the reasons for increased fraud exposure. Even so, the sector has modest plans to invest in staff training and due diligence over the next 12 months.
Technology, Media and Telecoms	Moderate	Moderate	While the TMT sector continues to feel highly vulnerable to IP theft and information theft, loss or attack, there are a new and growing set of frauds that the industry needs to address: procurement fraud, financial mismanagement and corruption. Despite these increasing threats, investment in anti-fraud measures is only average compared to other sectors, and is primarily concentrated on IT security.
Consumer Goods	Moderate	High	This year, consumer goods companies saw a decline in the traditional risks areas associated with the sector – theft of physical assets, information theft, loss or attack and financial mismanagement. At the same time, it experienced a rise in vendor, supplier and procurement fraud, corruption, and internal financial fraud. The sector is aware of the challenges brought on by high staff turnover and is handling it appropriately. More consumer goods companies plan to invest in staff training than any other sector. The industry also has the second highest percentage, after financial services, putting new money into background screening.
Healthcare, Pharmaceuticals and Biotechnology	Moderate	High	This was a challenging year for the healthcare, pharmaceuticals, and biotechnology sector. On average, companies lost 2.6% of revenue to fraud, the second highest figure for any sector. The sector faces much more diverse risks than previous years, with more companies now having to deal with procurement fraud, internal financial fraud and financial mismanagement. Companies in the sector are dealing with their challenges and currently adopt a variety of anti-fraud measures.
Professional Services	Low	Low	Professional services companies report the second lowest percentage of companies hit by fraud (after travel, leisure and transportation). Even so, the sector continues to struggle with persistent issues around IP theft and information theft, loss or attack, and are more likely to cite IT complexity as the leading cause of increased fraud exposure. Still, investment in anti-fraud strategies is low compared to other sectors, with a focus on reputation monitoring and IP/trademark protections.
Travel, Leisure and Transportation	Low	Low	Despite the lowest recorded level of prevalence of any sector, travel, leisure, and transportation companies this year reported a marked increase in fraud exposure and saw a rise in five of the 11 frauds covered in the survey. However, lower incidence levels may be leading to complacency when it comes to investment in anti-fraud measures. The industry has the smallest percentage of companies planning to invest in information security, financial controls and physical asset security.

Key regional contacts at Kroll

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

Business Intelligence and Investigations

Tom Hartley
Global Head
London
44 207 029 5000
thartley@kroll.com

Americas

Robert Brenner
Vice President
1 212 593 1000
rbrenner@kroll.com

North America

David Holley
Boston
1 617 350 7878
dholley@kroll.com

Jeff Cramer
Chicago
1 312 345 2750
jcramer@kroll.com

Jack Weiss
Los Angeles
1 213 443 6090
jweiss@kroll.com

Richard Plansky
New York
1 212 593 1000
rplansky@kroll.com

Bill Nugent
Philadelphia
1 215 568 2440
bnugent@kroll.com

Betsy Blumenthal
San Francisco
1 415 743 4800
bblument@kroll.com

Peter McFarlane
Toronto
1 416 682 2784
ext. 3516
pmcfarlane@kroll.com

Douglas Franz
Washington
1 202 999 9382
dfrantz@kroll.com

Latin America

Andrés Otero
Miami
1 305 789 7100
aotero@kroll.com

Matías Nahón
Buenos Aires
54 11 4706 6000
mnahon@kroll.com

Andrés Otero
Bogota
57 1 742 5556
aotero@kroll.com

Glen Harloff
Grenada
1 473 439 7999
gharloff@kroll.com

Ernesto Carrasco
Mexico City
52 55 5279 7250
ecarrasco@kroll.com

Frederico Gebauer
São Paulo
55 11 3897 0900
fgebauer@kroll.com

Asia

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

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

Richard Dailly
Mumbai
91 22 6724 0500
rdailly@kroll.com

Feng Lu
Shanghai
86 21 6156 1700
flu@kroll.com

Abigail Cheadle
Singapore
65 6645 4942
acheadle@kroll.com

Penelope Lepeudry
Singapore
65 6645 4941
plepeudry@kroll.com

David Wildman
Singapore
65 6645 4520
dwildman@kroll.com

Tadashi Kageyama
Tokyo
81 3 3509 7100
tkageyama@kroll.com

Europe, Middle East & Africa

Tommy Helsby
London
44 207 029 5000
thelsby@kroll.com

Brian Stapleton
London
44 207 029 5126
bstapleton@kroll.com

Richard Abbey
London
44 207 029 5153
rabbey@kroll.com

Omer Erginsoy
London
44 207 029 5226
oerginsoy@kroll.com

Ben Hamilton
London
44 207 029 5071
bhamilton@kroll.com

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

Melvin Glapion
London
44 207 029 5313
mglapion@kroll.com

Brendan Hawthorne
London
44 207 029 5482
bhawthorne@kroll.com

Tom Everett-Heath
Dubai
971 4 4496701
teverettheath@kroll.com

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

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

Alfonso Barandiarán
Madrid
34 91 310 67 20
abarandiaran@kroll.com