Fraud in a downturn

A review of how fraud and other integrity risks affect business

PricewaterhouseCoopers

Contents

Introduction

The impact of the credit crunch and the global economic slowdown is challenging even our most robust institutions. Those charged with the governance of some of the largest private sector companies have had to focus on short-term measures to address the risk of corporate failure. Leaders of public sector institutions must confront challenges around guarding against fraud, corruption, waste and abuse in implementing multi-trillion dollar stimulus programs and maintaining and improving service provision when the resources necessary to deliver services may not be made available. The dilemma public and private organizations face is how best to manage recovery in the short-term, while not losing sight of the need to maximize shareholder value and to maintain and develop services over the medium and long-term.

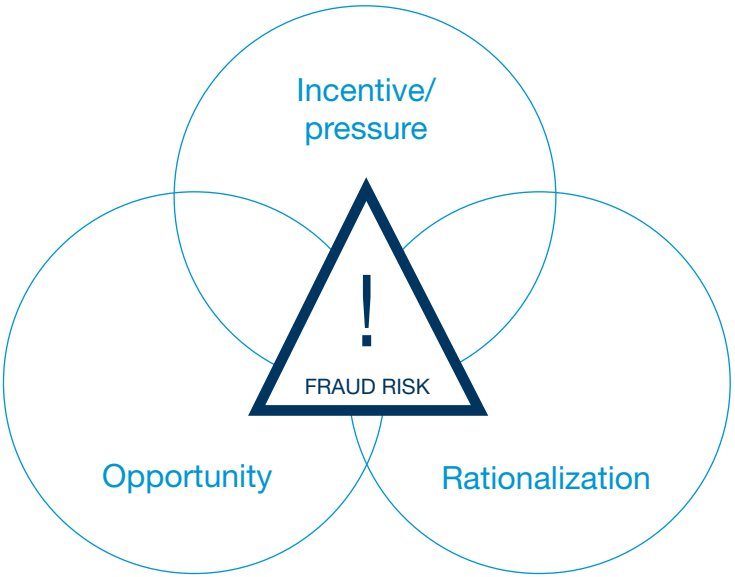
As the economy declines, both in the US and globally, new threats emerge. The recent collapse of certain investment schemes illustrates how allegations of fraud, previously undetected, emerge from the shadows. Possibly the only positive aspect of the credit crunch is that, as providers of finance retrench and seek return of loan finance or investment capital, fraudulent borrowing or fraudulent investment management is revealed, thereby capping the losses that have occurred.

When economic survival is threatened (either for the organization or for the individual) the line separating acceptable and unacceptable behavior can, for some, become blurred. In addition, fraud and other economic crime have become a focus of criminal activity over the past five years; criminal organizations that profit from fraud view the current economic conditions as an opportunity, not a threat.

This paper considers whether fraud, corruption, abuse and other integrity threats are changing during this period of economic decline and, if so, how. Looking forward, we consider the issues that boards of directors and audit committees need to beware of: the frauds that may emerge and the likely regulatory response. Finally, we describe the strategies proactive organizations are implementing to manage short term risks and enhance stakeholder value in the longer term.

The perfect storm

The Fraud Triangle, developed by the criminologist, Dr. Donald Cressey, describes three conditions that are commonly found when fraud occurs. The perpetrators experience some Incentive or Pressure to engage in misconduct. There must be an Opportunity to commit fraud and the perpetrators are often able to Rationalize or justify their actions. The global economic decline is such that each of these three factors (Incentive/Pressure, Opportunity and Rationale) is present as never before.



Incentive/pressure

While misconduct can, from a legal perspective, be perpetrated by a company, the steps taken to commit fraud are always the actions of individuals. It is sometimes assumed that people commit fraud for personal gain and in particular to obtain money. People are said, for example, to 'cook the books' in order to earn the large year-end bonus. The reality is far more complex. Personal gain is often a factor, in other instances it is personal reputation, pressure from above or a desire to help the organization succeed that can be the principal motivation.

Avoidance of loss, whether it be future income, job security, power or prestige is perhaps the strongest motivator. As people lose their jobs, and those still in employment feel ever more threatened, the pressure to commit fraud will increase. The majority of people are fundamentally honest and, as such, are not tempted by wrongful personal gain. However, when someone's livelihood is at stake, or the future of a company rests on obtaining a new order from a potential customer, some people will feel more acutely the pressure to do the wrong thing: to pay the bribe that secures the company's financial future or to look the other way while others do so.

Opportunity

Change presents opportunity and change, as we all know, is the only constant. What is new, however, is how the economic downturn is forcing the pace of change. Organizations looking to reduce costs must now do so with little time to reflect. Programs and projects are being cut at short notice. People are being let go without sufficient time for employers to reflect on the longer term consequences.

As change happens, gaps in the control system can and will appear. With fewer people employed there will be less scope for the segregation of duties, which is a key component of internal control in relation to fraud. In such circumstances checks and balances put in place to maintain control will be abandoned. Procedures whose purpose was to detect anomalies may be suspended.

Rationalization

The third element of the fraud triangle is the ability of individuals, be they front line operations staff or members of the board of directors, to rationalize the fraudulent act. To illustrate what we mean by this, below are some examples of rationalization, with a particular emphasis on themes that are almost certain to emerge as the economic downturn persists.

"Everyone pays bribes to make sales in that country, there is no other way."

"If the investment bankers can keep their million dollar bonuses, why can't I have a piece of the action?"

"Cooking the books or 'creative accounting' is not fraud; it is just bending the rules."

"This company is fundamentally sound—if I have to cross the line to get us through the next six months, so be it."

"I was entitled to a bigger bonus than I received, so I made up a bit of the difference via expense claims."

In difficult economic times the capacity for people to rationalize fraud and corruption increases.

Fraud and integrity risks

We have discussed the likely influence of the economic downturn on fraud. Given these circumstances, what are the likely effects on corporates, investors, regulators and government? The questions below are ones that we believe boards and audit committees should be asking themselves and key stakeholders:

1. Is your organization at risk of DOJ, SEC or foreign government scrutiny for public and commercial bribery in the US or overseas?

The Department of Justice (DOJ) and Securities and Exchange Commission (SEC) continue to clamp down hard on corruption.

While many companies have taken steps to create the right global anti-corruption policies, too few have put the right processes and controls in place to prevent corruption from occurring. There remains significant opportunity within some global organizations to engage in bribery (e.g. via 'consulting' payments or benefits in kind). Incentive (to win new business) and the ability to rationalize (it's 'market practice') also remain high.

2. How much are fraud and abuse losses in the supply chain and through revenue leakage costing your business? How much can companies recoup by taking the offensive?

We continue to be surprised by how few organizations understand what fraud is actually costing their businesses. It remains relatively rare for businesses to have a proper understanding of the fraud risks within their procurement process or to have designed controls to address these risks.

Fraud losses will continue to run at high levels. Some commentators put the estimate of losses from fraud at 7% of revenue.[1] We consider this figure to be high as an estimate of the impact of fraud on businesses in general, but we recognize that some companies will experience significant frauds that result in losses at this level, particularly in high risk frontier and emerging markets. We see continuing opportunity for significant fraud losses as many organizations continue to underestimate avoidable fraud losses and fail to develop adequate controls.

Proactive risk management is good for business. Studies show that effective management of fraud, corruption, waste and abuse produces an 8:1 return on investment[2], and strong anti-fraud controls reduce fraud by at least 30 percent[3]. So not only is legal risk mitigated, but the bottom line should increase from improved operating efficiency, reduced spending, and asset preservation.

[1] Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse.

[2] Nelsestuen, Rodney, *Enterprise Fraud Management in Financial Services: Restoring Confidence in an Uncertain World*, Tower Group, September 2007.

[3] Kielstra, Paul, *Global Fraud Survey*, The Economist Intelligence Unit, 2008.

3. How well does your organization know the people with whom it does business?

More and more, organizations are being held accountable for the actions of agents, suppliers, and other counter-parties. Regulators are prosecuting companies and their directors and officers for the inappropriate actions of business partners such as distributors and sales agents. Companies cannot simply ignore the actions of business partners who may be willing to pay bribes in order to achieve sales, but many still do.

Risks lie not just in the sales channel but also in the supply chain. Organizations in many industries have suffered reputational, legal and financial loss due to fraudulently concealed unethical practices arising in the supply chain including:

- agents paying commercial and public bribes
- suppliers failing to pay rebates
- the use of child labor by sub-contractors
- the failure of sub-contractors to properly vet employees working with children and in other sensitive industries
- sub-contractors sourcing materials from non-sustainable sources

Some organizations are beginning to address these risks and are using techniques akin to investigative journalism to conduct integrity diligence on business partners, but others are not. We see continuing high levels of opportunity for this type of fraud. Many organizations face significant reputational risk from inadequate due diligence and monitoring controls in relation to business partners in the sales channel and supply chain.

4. Is your organization at risk of a significant data theft?

In the past, discussions around fraud, integrity and asset losses have tended to focus on cash, tangible assets (e.g. stock/inventory) and financial securities. In 2007 and 2008, the losses of personal data experienced by public and private sector organizations were widely reported.

To date, most serious losses of personal data appear to be the result of mishap, not serious fraud or misconduct, although there have been some exceptions. Criminal organizations have for some time recognized the value of personal data and, while bank account details continue to have a black market value, there will be a significant risk of theft.

We see the principal threat arising from opportunity resulting from the inadequacy of control. In our experience, many organizations have begun to put arrangements in place to improve privacy and data security. However, not enough is being done to address the risk of deliberate theft by criminal organizations working in collusion with permanent, short-term or temporary staff to infiltrate organizations and circumvent existing control systems.

5. How robust are your controls in treasury and banking operations?

We tend to think of rogue traders as a threat faced only by investment banks. In fact, many organizations use hedging strategies in their treasury function or trade in energy or other commodities. The losses reported by Société Générale in 2008 were, perhaps, an early warning of the impact of a declining economy on the heightened risk of fraud and irregularity. As in so many cases, it appears that problems escalated as Jerome Kerviel, the trader at the center of the case, contrived to trade beyond his authority level.

We see increased opportunity for rogue traders to operate undetected as control environments weaken. There are also significant influences that will provide pressures or incentives for some staff to trade beyond the limit of their authority and rationalize their actions.

In addition, as companies sail ever closer to banking covenant breaches, the temptation to 'massage the numbers' provided to its banks (even if only designed to 'tide us over for a couple of months before that new contract is renewed') will increase.

Asset-based lending has allowed companies to obtain debt finance while enabling lenders to secure lending against specified company assets. The range of assets against which debt can be secured ranges from the more traditional (stock/inventory, debtors, property, plant and equipment) through to the more unusual such as intellectual property assets (trademarks, patents, franchise and design rights). As credit becomes ever harder to obtain, we see a significant increase in the incentives and pressures of borrowers facing difficult trading conditions to commit frauds and also the ability of at least some borrowers to rationalize their actions. We also see the pressures on the asset-based lenders to control their own costs constraining the resources they can apply to counter this threat.

6. Is your organization at risk of breaching competition laws?

In 2008 the Justice Department and Federal Trade Commission pursued a proactive regulatory stance in relation to the investigation and detection of anti-competitive cartel practices, as have the European Commission, UK Office of Fair Trading and Chinese government. Total fines were in the billions of dollars and we expect this to continue. Many companies have yet to consider price fixing risks as part of their fraud and integrity risk assessment or to develop policies and programs to address this risk. Many fraud and integrity risk training and education programs focus solely on corruption risks, to the exclusion of other integrity related issues. There is therefore significant opportunity for this kind of irregularity. Ability to rationalize is also high as, despite recent high profile fines and the prosecution and imprisonment of individuals, many still do not yet see price collusion, bid rigging and market sharing as forms of fraud.

The regulatory fines that can be levied for price fixing are substantial (up to 10% of turnover) and the reputational risks that organizations face are significant. We expect more companies to be prosecuted for anti-competitive behavior and to incur significant financial penalties and reputational damage as a consequence. This is likely to result from a whistleblower seeking leniency from the regulator, given the attractive leniency programs and financial rewards for making such disclosures.

7. Is your organization at risk through the way it recruits and downsizes?

We anticipate that the number of people providing misleading information in order to obtain employment will rise as competition for jobs becomes more intense. Providing false qualifications or references, and with-holding information that may be detrimental to an application including hiding criminal convictions are common, particularly as the unemployed take lengths to obtain employment.

Downsizing, unless carefully planned and managed, skyrockets internal and external misconduct risks. Eliminating positions often eliminates critical segrega-tion of duties. Even segregation occurs on paper, so fraudsters can easily evade thinly spread or disillusioned remaining employees. We have seen “good” employees engaging in fraud to cover up innocent mistakes in fear of being the one selected for downsizing.

The economic decline will, for some individuals, increase their motivation and ability to rationalize misconduct. We also foresee increasing opportunity as back office headcount is reduced.

Which industries could be affected the most? Unlike in previous recessions, this downturn appears to be hitting the services sector as hard as manufacturing, or even harder. Service providers including banks, law firms and accountants all face increased threat levels.

8. How strong is your first line of defense?

Operations and finance personnel compose the first line of defense against fraud, corruption, and abuse. Legal, compliance, and internal audit functions form a critical, but last line of defense. Because most compliance, internal audit and legal departments are one step, if not two or three steps removed from the day-to-day business, it is not wise to rely exclusively on them as the principal line of defense.

Viewing misconduct management as a “discretionary spend”, we now see organizations retreating from efforts to equip front line personnel with antifraud knowledge, skills and tools. Is this penny wise and pound foolish? Organizations must demonstrate that they have taken reasonable steps to guard against fraud, corruption, waste and abuse. Expect little sympathy from regulators, investors, journalists and overseers when misconduct occurs, which could have prevented or more timely been detected, if front line personnel were more fraud savvy.

9. How well does your organization employ data analytics to prevent and detect misconduct?

The public and private sector, with notable exceptions, until recently has not employed data analytics as a tool to prevent and detect fraud, corruption and abuse. Fraud experts attribute lack of use to (i) challenges in collecting and analyzing data, and (ii) a general reactive approach.

Fraud and forensic technologists theorize that fraud, corruption and abuse result in some data anomaly. The challenge lies in identifying risk indicators which do not give rise to an excessive number of “false positives”.

We predict that companies will be able to rely more heavily on data analytics. Data collection and analysis has become less expensive and simpler, particularly with the development of common data platforms, which allow forensic technologists to compare data housed on incompatible information systems or in foreign languages such as Chinese and Arabic.

PwC employs an advanced analytics tool to analyze detailed transactional data in general ledgers for indicators of fraudulent financial reporting. The tool considers the entire data population as opposed to statistical samples. Rather than search for traditional red flags, the tool applies algorithms to detect anomalies.

Boards, senior management, investors, law enforcement and other stakeholders expect companies to take the offensive against fraud, corruption and abuse. When misconduct occurs, the government and other stakeholders will ask why the organization did not detect the incident earlier. The organization faces embarrassment and possibly tougher sanctions, if it turns out that red flags were overlooked.

To leverage data analytics, companies need to ask:

- What are significant vulnerabilities?
- Have we identified key risk factors and indicators?
- Can analytics be used to identify risk factors and indicators?
- What analytics can we develop to timely detect factors and indicators?

10. How reliable is your financial data?

Where senior managers have colluded with third parties to misrepresent financial information and statements, fraud can be difficult to identify. Audit committees should consider whether internal controls and processes are sufficiently robust to prevent accounting fraud and ask some key questions:

- How strong is the ethical tone at the top and in the middle?
- Is there adequate segregation of duties and responsibilities?
- Are remuneration systems driving the right behaviors?
- Is the segregation of key duties and responsibilities still adequate following any cost cutting initiatives?
- Do we have an adequate whistleblower hotline and would employees speak up if they had concerns?
- How well resourced is internal audit, compliance and other third lines of defense?
- Does internal audit have the necessary fraud detection experience?
- Do we have the necessary financial skills to challenge the numbers?

11. If a crisis occurred, how well prepared are you to react?

We expect both the DOJ and SEC to continue their respective adoption of a more proactive approach to the detection and investigation of fraud and regulatory breaches. Prosecutors and regulators expect organizations to implement effective controls over criminal conduct just as public companies must have effective controls over financial reporting.[4] The Government expects—and, for government contractors, requires—that the company:

- identify and assess criminal conduct risk
- evaluate design and validate operating effectiveness or preventive and detective controls
- conduct monitoring and auditing to detect criminal conduct

Companies must report, at an early stage, if a regulatory breach, fraud or corruption is identified. Those that do not and eventually get found out receive harsher sanctions and, if a government contractor, face potential suspension or disbarment from doing business with the government.

Companies need to be 'investigation ready', i.e. they will need to have policies in place regarding the conduct of investigations and will be expected to know where data is stored and how it can be speedily retrieved.

Companies must also demonstrate that they have taken action to prevent recurrence, beginning with ring-fencing the issues to understand whether the perpetrators engaged in other, unrelated wrongdoing or whether similar misconduct occurred elsewhere in the organization. The organization needs to conduct root-cause analysis: did the misconduct result from a poor control environment, inadequate risk assessment, poor preventive controls and/or weak detection processes?

As well as criminal prosecutions, regulators are making more use of their ability to seek civil penalties in order to dispose of some cases. In seeking to resolve investigations in this way, regulators will take into account:

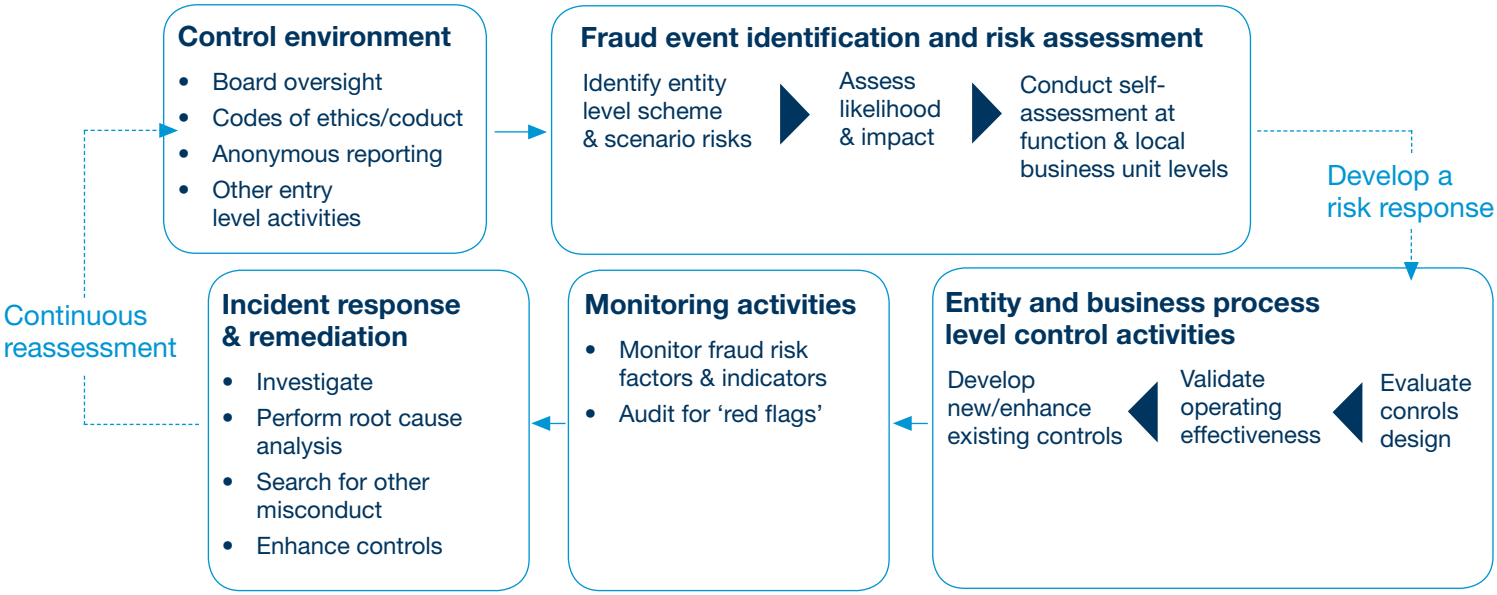
- the steps taken before the incident to identify the risk, develop controls and conduct auditing to detect misconduct
- the rigor with which an organization reacted to an alleged incident including the thoroughness and independence of any internal investigation
- the quality and comprehensiveness of the organization's efforts to conduct a root cause analysis and implement and monitor controls to prevent recurrence
- the cooperation afforded them by the company

[4] For a side by side comparison of US Sentencing Guidelines and Sarbanes-Oxley requirements, see Frank, Jonny, "Leveraging Sarbanes-Oxley Efforts to Meet USSG Requirements Ethics and Compliance Program Requirements," *The Conference Board Corporate Governance Handbook*, 2007.

The strategy of the proactive organization

One hears commentators on fraud describing how a particular solution is key to the management of fraud risk—'risk identification,' 'the tone at the top' or 'better use of technology' are just a few of the many keys that seem to be available. In our experience the proactive organization evaluates the options available to reduce fraud losses within a detailed framework.

The PwC antifraud framework[5]



[5] In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a model for evaluating internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control. We have adapted the COSO framework to illustrate some of the key elements of a fraud and integrity risk control framework.

The strategy of the proactive organization (Cont.)

Each organization must determine how best to implement a fraud and integrity risk strategy. We set out below some of the questions those charged with governance need to ask, and receive answers to, in order to obtain some comfort that a sound strategy is in place:

- Organizational tone—what steps are being taken to be certain that the right tone at the top permeates down through the organization? Does our remuneration strategy, including bonus arrangements, support the organization's ethical stance, or undermine it?
- Management information—does middle and senior management have the knowledge, skills and tools they need to manage fraud and integrity risks?
- Communication and training—do our people receive proper communication and training? Are operational and finance staff an effective first line of defense against fraud and integrity risks?
- Risk identification—how does management identify fraud and misconduct risk? Who is making this assessment and what information is the assessment based on? What input is received from business unit and function leaders - the first line of defense? Has anyone thought through the fraud and integrity risks arising from the people we do business with, i.e. our sales agents, distributors, joint venture partners and supply chain?
- Control linkage and evaluation—is the control system designed principally to identify errors or is it sufficiently robust to prevent or detect fraud, corruption or other misconduct risks? Are we using leading practice unpredictable controls, including spot checks and data mining, to help both detect and deter potential fraudsters?
- Preventive controls—does management leverage the "fraud triangle" (incentives/pressures, opportunities, rationalization) to develop preventive controls? Does controls evaluation consider vulnerability to override, collusion, unauthorized access and other forms of circumvention?
- Monitoring and auditing—has management identified key risk factors and indicators? What process do management and internal audit use to identify key risk factors and indicators? How well does the organization employ data analytics?
- Incident response and remediation—what is the process for triaging allegations or suspicions of fraud and corruption? Are we conducting thorough, independent investigations? How well do we analyze the root cause of misconduct and enhance/monitor controls to prevent recurrence?

Conclusion

The economic downturn is changing the nature and scale of fraud and integrity risks that organizations face. The speed of change is such that opportunities to commit fraud will be prevalent. More people will feel real pressure to 'cross the line' or to look the other way while others do so. In addition, the falling economic tide will expose more frauds that have been ongoing while economic conditions were good. Although there are many competing priorities for those charged with governance to consider, in our view boards of directors would be wise to reflect carefully on the changing landscape of fraud and other integrity risks.

It is for those charged with governance to take the lead and demonstrate that fraud and integrity are critical *business issues*—not just legal and compliance issues. Employees look to the board and senior management to set the tone and unless the senior commitment is there, change will not happen and the benefits of reducing fraud and other integrity risks will not be realized.

The good news is that effective fraud risk management more than pays for itself. Companies across industry sectors are desperate to find ways to reduce cost. Attacking fraud, waste and abuse offers a huge cost savings opportunity for a relatively low investment.

The challenge organizations face is that there is no single 'key' to stopping fraud and misconduct. Organizations need to develop a strategy that enables the deployment of appropriate measures to manage this increasing risk. The strategy needs to be owned by front line personnel; otherwise it will not succeed. Most large organizations have mature legal, compliance and internal audit functions. But these are one step removed from where the fraud and misconduct occur. Front line operations and finance personnel need to become effective first and second lines of defense.

PwC has developed a self-assessment tool for organizations to benchmark their fraud and integrity risk program. Please contact the author of this white paper if you would like to know more.

About PwC Forensic Services

Fraud prevention and detection experience:
Fraud specialists face the daunting task of discovering misconduct in the absence of an allegation. Just as doctors need medical manuals, fraud specialists require knowledge of the various ways that misconduct is committed, prevented and detected. PwC has invested over 100,000 hours researching common, sector- and market-specific misconduct schemes involving fraudulent reporting, asset misappropriation, and criminal conduct. PwC risks and controls professionals developed manuals detailing the mechanics, controls, risk indicators and detection procedures for hundreds of fraud scenarios, which are tailored to specific client needs and circumstances.

Thought leadership: PwC is a thought leader in prevention, investigation and remediation of fraud. Hundreds of companies have used our anti-fraud framework—which has been embraced by COSO, SEC, IIA, and the AICPA—to benchmark the effectiveness of efforts to guard against misconduct. We have published numerous fraud prevention whitepapers, beginning with the seminal *Key Elements of Anti-fraud Programs and Controls* published in 2003 and continuing with industry specific guides. Related publications include *Confronting Corruption**, *The Business Case For An Effective Anti-Corruption Programme*, and PwC's *Biennial Global Economic Crime Survey*.

Global reach and trustworthy brand:
PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services to build public trust and enhance value for its clients and their stakeholders. More than 155,000 people in 153 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

Author:

Jonny Frank
jonny.frank@us.pwc.com
Tel: +1 (646) 471 8590

Contact us:

Boston
Erik Skramstad
erik.skramstad@us.pwc.com
Tel: +1 (617) 530 6156

Dallas
Charles Reddin
charles.reddin@us.pwc.com
Tel: +1 (214) 754 5173

Chicago
Kevin Kreb
kevin.kreb@us.pwc.com
Tel: +1 (312) 298 2587

New York
Manny Alas
manny.a.alas@us.pwc.com
Tel: +1 (646) 471 3242

Philadelphia
Chris Barbee
chris.barbee@us.pwc.com
Tel: +1 (267) 330 3020

San Francisco
James Meehan
james.r.meehan@us.pwc.com
Tel: +1 (415) 498 6531

pwc.com/us/forensics

© 2009 PricewaterhouseCoopers LLP. All rights reserved. “PricewaterhouseCoopers” refers to PricewaterhouseCoopers LLP, a Delaware limited liability partnership, or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.