

# Confronting Fraud in a Downturn

## Old Scams and Evolving Risks

The global economic downturn and uncertainty in market conditions have created an environment that both exposes existing financial scams and engenders new frauds.

*by Richard Abbey, Alan E. Brill &  
Brian G. Lapidus*

With banner headlines publicizing massive frauds around the world, individuals and businesses are paying increased attention not only to investments but also to questionable operations. Swindles that rely on a continuous supply of new victims are harder now; people have less money to invest and often switch to safer investments. Furthermore, companies watching costs are more likely to investigate unusual spending. As old frauds come to light and regulatory bodies inevitably take action, businesses can benefit by anticipating and preparing for the consequences.

At the same time, increased competition for fewer opportunities is straining ethical boundaries. Economic difficulties can change the behaviors of normally trustworthy people. Some individuals facing intense financial pressure will resort to crime, driven by desperation or unwillingness to make lifestyle adjustments.

Those with responsibility for a company's finances may be tempted to become "corporate saviors," massaging figures in a misguided attempt to save a struggling business. They may conceal the company's true financial position in order to prevent staff reductions, cover up breaches of banking covenants, obtain credit from suppliers, or raise new debt or equity. Often these individuals believe that falsifying financial statements will be only a temporary measure until business improves. Frequently, however, the fraud has to grow as the company continues to lose money.

As businesses deal with the difficult decision to reduce staff headcount, employee morale and data security must be addressed. Employees who feel slighted may be more tempted to misappropriate intellectual property or personal information from employees or customers. Tightening budgets are causing some companies to cut back on data security measures, even though proprietary data and personal information is at increased risk.



Regardless of the motivation for fraud, companies must consider how to protect themselves, how to detect and investigate malfeasance, and the regulatory obligations that arise.

## Preventing fraud

### Enhanced due diligence

Institutional and private investors alike have been shocked to discover that they have been duped by trusted professionals with strong track records. Thorough investment due diligence is important; however, it is only one aspect of comprehensive fraud risk management. A broad approach to due diligence – rather than a “check-the-box” review – is not only vital to managing risks through the economic downturn, it greatly assists effective day-to-day business operation. Businesses must ensure that they have sufficient knowledge about prospective employees, business partners, third parties, and transactions.

With economic distress contributing to business closures and job loss, ensuring the authenticity and integrity of front-line employees and executive leadership is critical. As always, new applicants should be screened to verify identity and work history claims, as well as to discover any criminal record that might block employment. Ongoing screening at achievement points (promotion, additional access to confidential information, etc.) or at timed intervals will decrease the potential for a new risk to arise and remain undetected.

Components of partner relationships and transactions, such as individual employees, principals, and business entities, require analysis to prevent possible negative effects on revenues or reputation. Businesses should not feel safer in certain countries; this is a global issue relevant to all industries. International due diligence can



be challenging, but need not deter investments abroad or entry into new markets. Comprehensive, compliance-driven investigations can provide crucial information on important decisions, providing lasting business benefits.

Finally, businesses must screen third parties who will work on company property, alongside personnel or directly with clients. It is not unreasonable to expect vendors to mirror the company's existing screening standards, providing an extra layer of protection from possible risk.

### **Monitoring and corporate governance**

Internal controls, no matter how good on paper, will be ineffective if improperly implemented or monitored, or if collusion within an organization allows them to be bypassed. Supervision is fundamental to reducing opportunities for dishonest behavior and ensuring that possible fraud is flagged early. Those responsible for managing fraud risks must thoroughly understand the business and its people, particularly in overseas or remote locations. Companies looking to shave costs on international operations must also be prepared to understand developments in the supply chain and how that may affect the business. For example:

- Senior executives must have a practical, hands-on understanding of how each division, as well as the company as a whole, makes money. A solely theoretical perspective may leave gaps in understanding whether reported revenues logically follow from the business activities.

- Risk managers, compliance teams, and non-executive directors should understand whether the profits align with trends in the global economy. They should ask questions such as: Why are we the only company in our sector generating such high/low returns? And, why does this star performer complain about internal audits? Red flags must not be ignored for fear of upsetting sales teams or senior management. While executives face constant pressure to generate increased profits, an overlooked fraud will be significantly more expensive in the long term.
- Financial institutions must ask: Do our senior managers and auditors really understand the products that are being traded and the attendant risks? In financial organizations, there is a great deal of scope for improper disclosure and misrepresentation. Trading products are highly sophisticated and often senior managers are not trained to use the technology, therefore relying on the knowledge of junior staff.

The economic downturn will also lead to tighter regulation. In the United States, for example, the Securities and Exchange Commission announced earlier this year that it will be increasing the severity of penalties it seeks for Foreign Corrupt Practices Act (FCPA) violations. The impact of an investigation – including legal costs, potential fines, and negative impact on market capitalization or reputation, can be devastating. Those contemplating foreign activity must therefore ensure that they take an FCPA-compliant approach, which includes: maintaining and adhering to



written policies and procedures, using risk-based metrics to determine the depth of the due diligence investigation, and engaging specialists to help obtain the information necessary to understand business operations fully.

## **Responding to fraud**

### **Whistleblowers, investigation and forensics**

The vast majority of fraudulent activity is uncovered by accident or through whistleblowers. Companies, therefore, must have an adequate framework to handle whistleblowers both internally and externally. They must investigate reports of unethical or fraudulent activity, clearly document how allegations were addressed, and create a summary of the outcome.

When a potential incident occurs, an internal investigation becomes necessary. The first order of business is to create an investigative team that includes counsel, a forensic accountant, and an investigator. The right investigator is often critical, requiring a combination of experience in the relevant kind of fraud investigation and a thorough understanding of the facts of the case. Additionally, most internal investigations will require computer analysis; if an investigation involves data collection and/or analysis, the investigator must have experience in proper forensic protocols.

Once formed, the team must quickly determine the likely key issues, and create a data map outlining the location of all potentially relevant information. This will also involve identifying key custodians of the data and how the company normally conducts business related to the

fraudulent activity. Evidence must be preserved in a way that protects its origin, integrity, and chain of custody. Preservation is often complicated by the involvement of personal computers or other types of electronic storage. Investigators must secure data from all sources in a defensible manner following proper forensic protocols in order to avoid tampering claims.

Interviews are often an essential part of a fraud investigation, but before proceeding the team should construct a timeline detailing the evidence and suspected players. This will provide a clearer understanding of what may have happened and permit more efficient questioning during interviews. Where relevant in the interviews, investigators should use information gained throughout the investigation to ask pointed questions, properly gauge answers, and establish if a witness is being untruthful or obstructive.

Applying best practices is vital in conducting a successful investigation into allegations of fraud. A sophisticated investigative team can increase a company's chances of determining who was involved in the fraud, giving a company a heightened chance to regain a portion of the losses and prevent future incidents of fraud.

### **Data breach notification**

When a fraud includes a breach of sensitive personal data – of employees, customers, or other constituents – a whole new audience demands attention. The response must be deliberate and prudent. An Incident Response Plan (IRP) should, among other things, identify an internal



team to manage the event, as well as establish a chain-of-command for investigation, assessment, and notification of required agencies and impacted individuals. The company should also preselect identity management products and services that can be deployed quickly to help those affected recover their pre-breach status and confidence.

Complying with diverse legislative requirements can be daunting. For example, one law might call for a detailed description of the event while another might simply require an approximate date of discovery. Few organizations face data breaches daily. It may be useful to engage an outside specialist with up-to-date knowledge of, and a proven record in, this complex area. Depending on the size, type and visibility of the organization, the IRP team might also benefit from crisis communications practitioners, to counsel team members and oversee the release of information to media and industry observers. Reputational recovery requires a concentrated effort to assure internal and external onlookers that the incident has been addressed, and all reasonable measures have been taken to halt further damage.

### **Looking ahead**

Corporate in-house and outside counsel are expected to be kept busy for the next few years as investigations and legal claims rise sharply. Companies need to focus not only on the immediate situation, but also on the likely long-term effects. If history is any guide, companies will see a substantial increase in fraud claims, legal disputes and regulatory actions. With increased litigation comes increasing data retention requirements.

Over the coming months and years, new regulations will likely be imposed on these companies, placing a bigger burden on already strained budgets and resources. Additionally, the majority of modern litigation involves at least a minimal amount of electronic discovery. Taking a proactive approach is vital. Pertinent members of the company's response team should know where data is kept and how it is maintained. Keeping communication lines open is also important to ensure everyone in the company remains on the same page. This will allow a more efficient and well-educated response to any legal discovery requests, audits or regulatory compliance requirements, which will ultimately help save time and money.

The economic downturn has brought old frauds to light and created an environment in which new risks can evolve. In these uncertain times, businesses must know where vulnerabilities lie, be prepared, and plan their responses accordingly.

---

*Richard Abbey is a London-based managing director of Financial Investigations at Kroll. He can be reached at [rabbey@kroll.com](mailto:rabbey@kroll.com).*

---

*Alan E. Brill, CISSP, CFE, CIFI, is a New York-based senior managing director of Computer Forensics at Kroll. His email is [abrill@krollontrack.com](mailto:abrill@krollontrack.com).*

---

*Brian G. Lapidus is the Nashville-based COO of Fraud Solutions at Kroll. He can be reached at [blapidus@kroll.com](mailto:blapidus@kroll.com).*