Fraud in a Downturn

A review of how fraud and other integrity risks will affect business in 2009

PricewaterhouseCoopers

Contents

Intro	4
Fraud and integrity risks in 2009	7
The strategy of the enlightened organisation	15
Conclusion	19

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 our 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 maintaining and improving service provision when the resources necessary to deliver services may not be made available. The dilemma public and private organisations face is how best to manage recovery in the short term, while not losing sight of the need to maximise shareholder value and to maintain and develop services over the medium and long term.

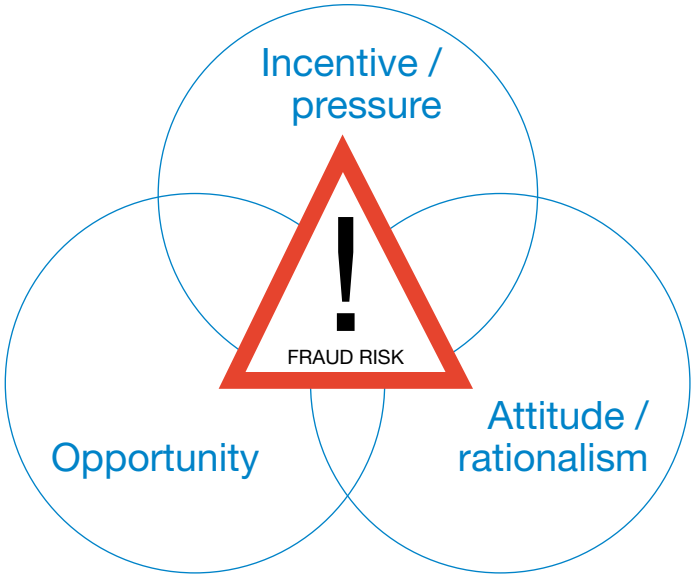
As the economy declines, both in the UK and globally, new threats emerge. The recent collapse of certain investment schemes illustrates how allegations of fraud, previously undetected, emerge from the shadows. Possibly the only positive aspect of the credit crunch is that, as providers of finance retrench 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 organisation or for the individual) the line separating acceptable and unacceptable behaviour 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 organisations that profit from fraud view the current economic conditions as an opportunity, not a threat.

This paper considers whether fraud and 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 in 2009: the frauds that may emerge and the likely regulatory response. Finally, we describe the strategies enlightened organisations are implementing to manage short term risks and to 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 **Rationalise** or justify their actions. The global economic decline is such that each of these three factors (Incentive / Pressure, Opportunity and Rationale) are present as never before.



Incentive / Pressure

While fraud 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 organisation succeed that can be the principal motivation.

Avoidance of loss, whether it be future income, job security, power or prestige can be a strong motivator. As people lose their jobs, and those still in employment feel ever more threatened, the pressure to commit fraud will increase. The great 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. Organisations looking to reduce costs must now do so with little time to reflect. Programmes 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 that 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 can be suspended.

Rationalisation

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 rationalise the fraudulent act. To illustrate what we mean by this we have set out below some examples of rationalisation, 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 city 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 made up a bit of the difference via expense claims."

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

Fraud and integrity risks in 2009

We have discussed the likely influence of the economic downturn on fraud in 2009. 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 the organisation at risk of regulatory scrutiny for bribing public officials in the UK or overseas?

The Serious Fraud Office has signalled its intention to clamp down hard on corruption. A new Head of Anti-Corruption has recently been appointed and it has been reported that the SFO has a portfolio of corruption cases. Many companies (or at least their senior employees) continue to believe it is necessary to pay bribes (or to use agents who have the right contacts at the right price) in order to compete in some emerging markets.

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 occurring. There remains significant **opportunity** within some global organisations to engage in bribery (e.g. via 'consulting' payments or benefits in kind), **incentive** (to win new business) and ability to **rationalise** (it's 'market practice') also remain high.

2. How much are fraud losses in the supply chain and through revenue leakage costing our business?

We continue to be surprised by how few organisations understand what fraud is actually costing their businesses. Too few retailers have reliable data on stock shrinkage. 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 in 2009. 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 recognise that some companies will experience significant frauds that result in losses at this level. We see continuing **opportunity** for significant fraud losses as many organisations continue to underestimate avoidable fraud losses and fail to develop adequate controls.

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

3. How well do we know the people we do business with?

More and more, organisations are being held accountable for the actions of the parties they contract with. 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. Organisations in many industries have suffered reputational damage due to fraudulently concealed unethical practices arising in the supply chain including:

- the use of child labour 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 organisations are beginning to address these risks and are using Corporate Intelligence techniques to conduct integrity due diligence on business partners, but others are not. We see continuing high levels of **opportunity** for this type of fraud. Many organisations face significant reputational risk from inadequate due diligence and monitoring controls in relation to business partners in the sales channel and supply chain in 2009,

4. Is the organisation 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 Her Majesty's Revenue and Customs and other organisations 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 organisations have for some time recognised 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 organisations have begun to put arrangements in place to improve data security. However, not enough is being done to address the risk of deliberate theft by criminal organisations working in collusion with permanent, short term or temporary staff to infiltrate organisations and circumvent existing control systems.

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

We tend to think of rogue traders as a threat faced only by investment banks. In fact, many organisations 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 centre of the case, contrived to trade beyond his authority level.

In 2009 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 **rationalise** 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 couple more 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 **rationalise** 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. Are we at risk of breaching competition laws?

In 2008 the Office of Fair Trading pursued a pro-active regulatory stance in relation to the investigation and detection of anti competitive cartel practices, as did the European Commission. Total fines were in the billions of euros and we expect this to continue in 2009. Many companies have yet to consider price fixing risks as part of their fraud and integrity risk assessment or to develop policies and programmes to address this risk. Many fraud and integrity risk training and education programmes 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 **rationalise** 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 organisations face are significant. We expect more companies to be prosecuted for anti-competitive behaviour in 2009 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 programmes and financial rewards for making such disclosures.

7. Are we putting the organisation at risk through the way we recruit?

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, withholding information that may be detrimental to an application including hiding unspent criminal convictions are common examples of the lengths that some people are willing to go to in order to obtain employment.

The economic decline will, for some individuals, increase their **motivation** and ability to **rationalise** this type of fraud. We also foresee increasing **opportunity** for recruitment fraud: as back office headcount is reduced, resources currently being devoted to pre-employment screening may be cut back.

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 reliable is our 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:

- Is the ethical tone at the top correct?
- Is there adequate segregation of duties and responsibilities?
- Are remuneration systems driving the right behaviours for our senior people?
- 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?
- Does internal audit have the necessary fraud detection experience?
- Are the reporting lines correct?
- Do we have the necessary financial skills to challenge the numbers?

Frauds that emerge in 2009 will have been begun in 2008 or even earlier with the economic downturn acting as the catalyst in the detection of the wrongdoing. As Warren Buffet so memorably, put it: "you only find out who is swimming naked when the tide goes out".[2]

9. How reliable is the non-financial data we provide to our stakeholders and regulators?

We have seen numerous instances of 'non-financial' fraud in 2008, involving the deliberate misrepresentation of disclosed information, for example non-financial performance data. Water and electricity utilities have become embroiled in cases of this kind in recent years, whereby allegedly misleading data has been provided to the relevant regulator. There have also been some examples of the deliberate misstatement of waiting list data within the health sector.

We see the principal threat of this type of fraud arising from the ability of some organisations and particular employees to **rationalise** the misstatement of non-financial data – often this type of behaviour is considered as harmless poetic license to achieve a particular objective, rather than the fraud on taxpayers or service users that it often amounts to.

[2] Letter to the shareholders of Berkshire Hathaway Inc., 28 February 2002

10. If a crisis occurred, how well prepared are we to react?

We expect both the Serious Fraud Office and the Financial Services Authority to continue their respective adoption of a more pro-active approach to the detection and investigation of fraud and regulatory breaches in 2009. Companies are now expected to report, at an early stage, if a regulatory breach, fraud or corruption is identified.

Companies will 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.

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 rigour with which an organisation reacted to an alleged incident including the thoroughness and independence of any internal investigation;
- the quality and comprehensiveness of the organisation's controls; and
- the cooperation afforded them by the company.

11. Do we have adequate Directors and Officers insurance?

Not withstanding the best internal controls, compliance programmes and 'fire-drills', it is sensible to ensure that the company carries sufficient D&O insurance to protect its officers and directors in the event of inward litigation and claims. Any exposure of the company to North America, especially via a US listing, significantly increases the risks of class action litigation whilst US regulatory investigations by the SEC or DOJ tend to be quite memorable for all the wrong reasons!

Prudent boards and audit committees will want to ensure via their broker that they have adequate insurance coverage.

The strategy of the enlightened organisation

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 enlightened organisation evaluates the options available to reduce fraud losses within a comprehensive framework of the kind we show below.

The PwC Fraud Wheel[3]

[3] 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 organisations 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.

Each organisation 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:

- **Organisational tone** – what steps are being taken to be certain that the right tone at the top permeates down through the organisation? Does our remuneration strategy, including bonus arrangements, support the organisation's ethical stance, or undermine it?
- **Governance** – are we receiving sufficient information and asking enough questions to have a sound strategic oversight of fraud risks, losses and prevention programmes. What are we doing personally to promote an anti-fraud culture?
- **Fraud and integrity policies** - do we have the right policies and practices in place (code of conduct, fraud policy, whistle-blowing, conflicts of interest, fraud response) and, more importantly, are they adequately publicised, promoted and enforced?
- **Hiring and promotion** – how much do we know about the people we recruit or promote to positions of responsibility? Is there anything else we should know before we bring them in or promote them?
- **Risk assessment** – what are the key fraud and integrity risks? Who is making this assessment and what information is the assessment based on? 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 best practice unpredictable controls, including spot checks and data mining to help both detect and deter potential fraudsters? Do we have a reliable, trusted whistle blowing programme (an essential anti-fraud and corruption control)?
- **Management information** – do our middle and senior management have the information they need to manage fraud and integrity risks? A sound information system will include reliable fraud loss reporting as well as data on ongoing internal investigations and whistle blowing activity.
- **Communication and training** – do our people receive proper communication and training? Are operational and finance staff an effective first line of defence against fraud and integrity risks? Have staff been trained to identify fraud and integrity risks in their business areas and to develop preventative and detective controls that really work?

The strategy of the enlightened organisation (Cont.)

- **Management oversight** - do senior management monitor fraud, corruption and other integrity based threats and take action where needed? Senior management should monitor compliance with key policies and the delivery of training programmes around business ethics.
- **Gatekeeper functions** – are teams working together in the right way to reduce fraud, corruption and other integrity risks? Are gatekeeper functions such as loss prevention teams, in-house legal, security, internal audit and the compliance function working together to deliver an effective fraud and integrity risk strategy?
- **Fraud and corruption response** – How well do we deal with allegations of fraud and corruption, when they arise? Are we conducting thorough, independent investigations and taking action where appropriate? How do we ensure that lessons learned from the investigation are implemented across the company, and not only in the area affected by the fraud?

Conclusion

The economic downturn is changing the nature and scale of fraud and integrity risks that organisations 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 whilst 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 on fraud and integrity 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 realised.

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 organisations face is that there is no single 'key' to stopping fraud. Organisations need to develop a strategy that enables the deployment of appropriate measures to manage this increasing risk. The strategy needs to be owned by those charged with governance, otherwise it will not succeed, and needs to involve people from across the organisation. Most large organisations 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 defence.

PwC has developed a self-assessment tool for organisations to benchmark their fraud and integrity risk programme. Please do contact any of the authors of this white paper if you would like to know more.

About PwC Forensic Services

The Forensic Services group of the PricewaterhouseCoopers global network of firms plays a lead role in addressing the lifecycle of fraud and other avoidable losses, providing reactive investigative services and proactive remedial and compliance services to clients in the private and public sectors.

The UK team comprises of over 200 dedicated partners and staff who specialise in areas such as investigations, fraud risk management, avoidable loss identification & mitigation, cost control, anti-money laundering, anti-bribery & corruption and corporate intelligence. The Forensic Services practice is supported by a team of forensic technologists who provide data mining and electronic discovery type services.

About the authors

John Tracey is a partner in the UK firm of PwC Forensic Services. He specialises in the investigation of complex fraud, corruption and other integrity issues. John leads PwC's Fraud Risks and Controls practice in the UK, advising clients on how best to manage fraud and integrity risks.

john.f.tracey@uk.pwc.com
Tel: 00 44 121 265 5783

Andrew Gordon is a partner in the UK firm of PwC Forensic Services and leads the investigations practice in the UK. Andrew is experienced in the investigation and remediation of a wide range of large, complex matters involving fraud, corruption and other misconduct.

andrew.gordon@uk.pwc.com
Tel: 00 44 20 7804 4187

www.managinginadownturn.com

Design Services 23300 (02/09).