Contents

Spring 2009

The Madoff scandal

An informer in the midst

Crunch time for auditors?

The intrusion test

Corporate fraud
The Madoff scandal

If it sounds too good to be true it probably is. This is the old maxim that investors and regulators seem to have failed to appreciate with the $50 billion Madoff fund, the largest Ponzi scheme in history, a scheme that by its nature could only survive by paying returns out of new investors’ monies. Madoff’s guilty plea in the criminal proceedings seems to confirm this.

Madoff’s fund gained a reputation for generating above average returns on a consistent basis year on year whether the markets overall were showing gains or losses. Apparently this was done by investing in US equities and using cap and collar arrangements. However, these arrangements normally only limit the upside and downside of an investment portfolio, not transform losses into consistently high profits. Remarkably Madoff had achieved only 7 small losses in a 14 year period. Madoff’s fund gained a reputation for generating consistent high profits. An arrangement of high commissions for introducing new investors and getting existing investors to put in more funds, and the appointment as auditor of relatively small audit firms.

In the US there are a number of class actions against Madoff’s companies, various hedge funds, fund managers, auditors, custodians and one against the SEC. It also appears that there may be similar actions in the UK on foot.

We have seen and investigated these sort of schemes before. Typically they are conducted in low regulatory environments but, in this case, events unfolded under the nose of the SEC and were perpetrated by the former chairman of NASDAQ, one of the key US investment markets. This raises (again) major issues regarding the effectiveness of the regulators in the US and by association in Europe. Another important characteristic of such schemes which we have observed before is the lack of independent involvement in the investment structure, particularly by custodians, administrators and investment managers. Other warning signs include the use of professionals who have inadequate experience in this field, the payment to introducers of high commissions for introducing new investors and getting existing investors to put in more funds, and the appointment as auditor of relatively small audit firms.

In the US there are a number of class actions against Madoff’s companies, various hedge funds, fund managers, auditors, custodians and one against the SEC. It also appears that there may be similar actions in the UK on foot.

“The benefits of a sensibly set up Whistleblower Hotline can significantly outweigh any associated risks. Every company should consider introducing or creating access to one.”

Hubert Baumgartner, Senior Manager, Germany

Feedback and f.o.c. subscription requests can be sent to jemma.gregory@mazars.co.uk

An informer in the midst

Many European countries, together with the United States, have legal regulations governing an employee’s right to file evidence of illegal or unethical behaviour that has come to the employee’s attention as a result of his employment. To ensure that the employee does not fear reprisals, he is protected by whistleblower legislation. The Federal Republic of Germany intended to introduce such regulation in a new Section of the German Civil Code (Bürgerliches Gesetzbuch), however the Federal Government postponed it, and with it, an opportunity in the fight against fraud.

What is a whistleblower? A whistleblower is a person who alleges misconduct, such as corruption. Usually, he or she acts out of conscience and contrary to widespread opinion, is loyal, motivated to protect the employer, and in so doing prevent risks such as the loss of jobs. However the act is often seen as one of treachery and the whistleblower is ostracised, deemed to have damaged the company by his or her actions. Too frequently the whistleblower’s “reward” will be the loss of employment and social status.

Why is a Whistleblower Hotline advisable? With the help of a Whistleblower Hotline, employees and other stakeholders can communicate on matters of misconduct in the company anonymously, with the benefit that potential risks to the company are identified early. Indeed, the effectiveness of a Whistleblower Hotline is often underestimated. Over 60 percent of all reported crimes were discovered thanks to information from an “informant”. This ratio is much higher than other methods of discovery, such as through the internal audit function, where the rate is about 15 percent. However, only 20 percent of German companies have such hotlines, even though practical experience has shown that 97 percent of incoming information to such hotlines is significant.

“Over the next few years we are likely to see more examples of major fraud emerging as perpetrators struggle to hide them in the accounting records. In fact, they may have occurred already but we don’t yet know about them. Forensic accountants like our team in Mazars will be watching closely to see where they can use their previous experience of complex fraud investigations to assist with identifying what has happened, the tracing of monies and subsequent recovery actions.”

Warwick Sabey, Director, UK
Crunch time for auditors?

As economies worldwide lurch into recession and more and more businesses inside and outside the financial services sector find themselves in difficulty, the threat of unprecedented levels of litigation looms large. In many countries, professional advisors, including auditors, will inevitably be increasingly exposed to claims as parties look to those with deep pockets to recover their losses.

The global liquidity crisis is proving challenging for many, particularly those entities dependent on re-financing their operations in the short term, or at risk of having their facilities withdrawn as their trading performance deteriorates. As trading conditions worsen and asset values diminish, the presumption that an entity will continue in operational existence for the foreseeable future may in certain cases no longer be appropriate. Combined with the increased difficulties companies and auditors face making and auditing estimates and judgements in the current market conditions, these factors could lead to serious financial reporting errors or judgements.

In January 2008 the UK Auditing Practices Board issued its Bulletin 2008/1 on “Audit Issues when Financial Market Conditions are Difficult and Credit Facilities may be Restricted”. This Bulletin provided guidance on matters that auditors may need to consider when conducting audits in the context of entities affected by the credit crunch (guidance that is just as relevant in the now wider reaching global recession).

We have considered the contents of 2008/1 in the context of our experience of claimant and defendant auditor negligence cases and set out below some of the areas where auditors may be (or are perceived to be) exposed:

- Going concern. Too often insufficient audit attention is directed to the fundamental basis on which financial statements are prepared: whether or not the going concern assumption is appropriate. In the current climate we would expect an auditor to perform extensive going concern procedures, and where financing is an issue, obtain much more evidence to support the going concern assumption.

- Post Balance Sheet Events (PBSE). Where the speed of change of the economy is rapid it is even more important that auditors perform a thorough PBSE review to cover the period between the balance sheet date and the date the audit report is signed. We would expect the auditor to have considered and documented any threats to going concern or the impact of ‘credit crunch’ issues, including financing arrangements.

- Fraud and error. As the economic downturn progresses, incentives to commit financial crime and fraud intensify. Management may come under pressure to achieve certain results to secure or extend borrowing facilities. Over-stretched employees may be motivated to defraud their employer to resolve their own personal financial problems. We would expect audit teams to have been on heightened alert for the possibility of fraud and error in the current economic climate, and to tailor their audit procedures accordingly.

- Valuation of assets. The value of assets may well have been impaired following the ‘credit crunch’. Where assets are required to be measured at fair value their valuation may prove difficult, particularly where trading in those assets has been severely curtailed or has even ceased and reliable market values are hard to determine. We would expect an auditor to have considered appropriately the basis of the valuation and whether the asset needed to be marked down to reflect the market conditions at the time, and where necessary, to have suggested that an expert valuation be obtained.

- Cash deposits. Where material cash deposits are held, we would expect an auditor to have considered the security and recoverability aspects relating to these deposits.

Crunch time? In these troubled times it seems inevitable that at some point the spotlight for recriminations will be very firmly on auditors. Over the coming period, many independent forensic accountants and other audit specialists are likely to be kept busy considering whether auditors dealt appropriately with the increased risks presented by the current financial crisis and opting as to whether the auditor actually or seemingly planned, performed and documented their audits appropriately to obtain adequate and sufficient audit evidence. Those auditors who have failed to do so really could be facing the crunch....

The intrusion test

When economic times are more difficult, chasing unbooked revenues or avoiding unexpected cash outflows can become a significant part of the role of the custodians of a business. It is therefore of utmost importance that a business’ computerised data should be as secure as possible in order to minimise such occurrences. A business’ data is exposed to a number of risks, including:

- The increasing inter operability of information systems and use of extended networking business models results in large amounts of data circulating between information systems, both secure and insecure, without distinguishing its nature (personal, banking etc.) or its importance (i.e. whether it should be accessible only to decision makers, a specific group, or everyone).

- Businesses are increasingly exposed to loss from and damage to information systems arising from targeted malicious attacks (viruses and hackers) as well as from natural disasters (floods, heatwaves, storms etc).

- The regulatory framework is increasingly restrictive. Beyond simple technical considerations (information system security, availability of data, confidentiality procedures etc) regulatory constraints force businesses to control their information systems.

In a survey that Mazars conducted last year (http://www.mazars.fr/presse/cp06_2008_risques-si.php), 35% of businesses admitted being strongly exposed (47% said they were moderately exposed) to risks linked to information systems. However the methods put in place by these businesses to manage these risks often appeared to be insufficient. For example, 38% of the businesses admitted to not carrying out an information systems audit.

Data stored on the information systems should be managed and secured both from a technical point of view (by the system itself) as well as from a contractual or regulatory point of view (by those in charge of internal control and legal/compliance).

One information systems audit technique we employ which has proved its worth to many of our clients is the intrusion test. The objective of the intrusion test is to make sure that data protection on a computer network has been correctly implemented and that the data is sufficiently protected against malicious attacks from hackers through the internet or even from within the firm.

We recently performed an intrusion test on the production network of a company that markets and distributes on a daily basis a large number of tickets. We proved through our intrusion test that there were weaknesses in the company’s data protection systems which enabled us to completely compromise the production network thereby allowing us to access the 600 ticket machines and, for example, to edit the tickets. After identifying these weaknesses we helped the company to come up with technical and organisational solutions to help them ensure that such weaknesses could not be exploited by unauthorised personnel.

“It is essential that a forensic accountant appointed to investigate allegations of professional negligence is appropriately qualified, with current audit experience and specialist expertise in the relevant industry.”

Jemma Gregory, Senior Manager, UK

“To respond to increasing demands for data protection, Mazars has developed a service to help our clients match the level of data security with the level of protection required by the owner of the data, or internal rules on information management or the law.”

Luc Marty, Partner, France
Corporate fraud

A Chinese perspective

Despite the Chinese government’s efforts to combat fraud and corruption, statistics emanating from Tsinghua University would suggest that fraud and kickbacks have totalled approximately 15% of China’s GDP in the past decade.

Multinational companies are often more exposed to frauds in China. Unfamiliar with the local language, culture or business environment, expatriate management usually relies heavily on “trusted” local management. Relationships (“Guanxi”) open the door to the Chinese market for these companies, but these relationships may subsequently lead to real problems, as “normal business practices” result in significant losses through fraudulent transactions and bribes.

“With a population of over 1.3 billion, China is a market that cannot be ignored. However, whilst the cost of fraud and corruption is often considered part of the cost of investment in China, it is a cost that for many multinational companies may prove considerable, including exposing them to regulatory fines and reputational damage.”

Annie Chan, Managing Director, Hong Kong

When we have been called in by US and European parented groups to investigate their operations in China, it is not uncommon for us to find bogus transactions used to cover up cash and expensive gifts made by the companies’ sales executives to certain third parties as “facilitation fees” for helping to secure business. Expensive gifts in many cases were also considered part of staff remuneration. Our investigations have often been triggered by whistleblowers or are issues identified through staff compliance training.

A further dimension is added where payments have been made that are potentially in violation of the US Foreign Corrupt Practices Act or local bribery laws, and in such situations the company may be liable to pay substantial financial penalties and may suffer serious reputational loss as a consequence.

So, our top recommendations to help multinational companies manage fraud risks in their Chinese operations are:

• Be professionally sceptical – “trust but verify”.
• “Know who you are dealing with” – know your customers, suppliers, distributors and your other business partners well. Have formalised vetting procedures.
• Set up and monitor a formal internal control system.
• Look out for red flags, items that are abnormal, such as significant cash transactions.
• Put in place an ethical corporate culture and a fraud averse environment.

An Irish perspective

The announcement by the Irish quoted Greencore plc that it had uncovered a significant and deliberate concealment of costs in its mineral water business will raise concerns with senior management in many companies around Ireland who will be asking themselves “Could this happen to us?”.

This is not the first time that a high profile company has suffered unexpected financial losses as a result of accounting irregularities that have arisen in the main from a breakdown in fundamental internal control procedures. But, in addition to the financial cost of such an event, the loss of reputation and shareholder and market confidence can also have a significant impact on the organisation. In most cases, the issues in question appear to have slipped under the radar of senior management, and the internal and external auditors.

So what controls and risk management procedures can organisations implement to minimise their exposure to such losses? As a starting point, the following fundamental controls should be in place:

• A lead-by-example culture of compliance should be established with best practice that filters down throughout the organisation.

• A clear fraud risk management strategy should be in place, devised following a comprehensive review of the organisation’s risk environment.

• The internal control environment should be stringent and not easy to manipulate or override. All key accounting processes should be subject to regular review and challenge by senior financial management. There must be sufficient segregation of duties in all core accounting processes throughout the organisation.

• It is important that there is a culture of regular and active involvement from head office at remote business locations, particularly where local management may be heavily incentivised by performance related bonus arrangements or previous owners are still involved in the business and subject to earn out arrangements.

• A recognition of the importance of the internal audit process to risk management. Afford it a direct reporting line to the board of directors. Of course, many businesses will not have the luxury of a dedicated internal audit team but such businesses should consider outsourcing this function to a third party or extending the scope of the external audit process to cover a review of areas of perceived risk or concern.

• An embracing of the external audit process as an important component of the risk management process. It is important that the audit methodology is a risk based approach, agreed between the auditors and the management team, or audit committee where existing, and focuses on the key business risks. The auditors should meet with management and the internal audit team on a regular basis.

“Whilst the prospect of irregularities will cause anxiety in boardrooms across the business community, a sensible approach to risk management and adherence to best practice in internal controls will significantly reduce exposure to losses from irregular accounting practices.”

Tom O’Brien, Partner, Ireland

Please get in touch...