

A fraudulent new year?

Having seen billions of pounds wiped off their value and investor and consumer confidence in them hitting an all-time low, banks are now facing a potentially ruinous increase in fraud. Neil Hodge reports

» THERE'S nothing like a massive financial scandal to remind internal auditors that fraud can evade themselves, managers, the board, investors and regulators – even when it appears to be endemic throughout the organisation's activities.

Bernard Madoff, a former chairman of the US Nasdaq stock market, was arrested and charged on 12 December with securities fraud, in what may be one of the biggest fraud cases yet after his hedge fund ran up US\$50bn of fraudulent losses. Madoff is alleged to have used money from new investors to pay off existing investors in the fund in a massive "Ponzi" scheme. The fraud only came to light after Madoff told at least three employees that the hedge fund business – which served up to 25 clients and had US\$17.1bn under management – was a fraud, "one big lie", and had been insolvent for years. If found guilty, US prosecutors say he could face up to 20 years in prison and a fine of up to US\$5m. Among the banks which have already been affected are the UK's RBS, Spain's Santander and France's BNP Paribas.

At the time of *Internal Auditing*

going to press, it was still unclear how long the fraud had been going on for, though there are suggestions that the US Securities and Exchange Commission (SEC), the US financial regulator, had been warned as far back as 1999 that Madoff was operating the world's largest Ponzi scheme.

Although the scale of such frauds is unusual, the case flags up that fraudulent activity can potentially be hidden in high-volume but low-value transactions that seem "normal", rather than in a few major transactions.

According to KPMG's *Fraud Barometer*, the banking sector has been the main target of a major spike in fraud coming to court in the first six months of 2008. Figures show that over £630m of fraud came to court across 128 cases, substantially up from £421m across 91 cases in the previous six month period, and of that more than half (£350m) was against the financial sector. The firm warns that the figures are likely to get worse as the full impact of the credit crunch unfolds.

The six-month high was fuelled in part by two big cases – an alleged £220m attempt to hack into Sumitomo »

"It's disappointing that many firms continue to underestimate the risk of data loss and identity fraud to their businesses and customers"



“Fraud by individuals within companies is widespread and – unusually – lower level employees accounted for more fraud than managers”

» Matsui Banking Corporation’s systems, and a £70m attempted fraud within HSBC’s securities services division. Yet even without these two cases, there was still over £60m of fraud against financial institutions coming to court in the first half of the year, compared to just £37m in the whole of 2007.

According to CIFAS, the UK’s fraud prevention service whereby members share data about identified frauds and potential risks, the largest banks have made 10% more reports about fraud attacks in the first ten months of 2008 than for the whole of 2007. In addition, the Association of Payment and Clearing Services (APACS), the UK trade association for payments, has revealed that online banking fraud losses are up nearly 200% in 2008.

The reports have also highlighted changes in fraud trends. For example, the KPMG report found that fraud by individuals within companies was widespread and that – unusually – lower level employees accounted for more fraud than managers, who are often

seen to be in a better position to defraud their organisations. Such evidence has prompted experts and regulators to suggest that financial firms need to re-examine their approaches to fraud detection and prevention, and that internal audit should alert managers that the business could potentially face new fraud risks that have previously not being identified or flagged as high-level.

Closer look

Andrew Clark, head of financial crime at professional services firm PricewaterhouseCoopers (PwC), says that “banks and other financial services organisations need to have a closer look at their business operations and ask themselves if they have identified the major risks, whether these risks should be reprioritised, and whether the controls they have in place to mitigate them are adequate. The credit crunch is making banks change the way they provide some services and how they offer them, and these operational changes may introduce new risks to the organisation.”

The UK’s financial services regulator has also warned banks and other organisations to make fraud risk a priority for 2009. On 25 November at the British Bankers Association’s (BBA) annual financial crime conference, Philip Robinson, the Financial Services Authority’s (FSA) financial crime and intelligence division director, outlined the key financial fraud risks that the regulator thinks the financial services industry is most likely to be hit by in 2009. Chief among these were increases in employee fraud, poor data protection leading to an escalation of consumer fraud, and new fraud risks caused by changes to the organisation and its systems following the economic downturn.

Robinson told attendees that “the motivations of and temptations on some people in the market may be affected by declining income streams and internal pressures to hit targets that have become harder and harder to meet”. As well as that, many people



French bank BNP Paribas has been exposed to Bernard Madoff’s Ponzi fraud

are facing “deteriorating personal circumstances, caused by increased mortgage or loan payments with less income”. The resulting pressures, said Robinson, can – and in the past have – “pushed honest people over the edge and can increase the possibility that people may be tempted to manipulate figures or accounts to project the image of false revenues, or actively steal money – or customer data – from the company. Are you sure this could not become a major fraud?”

Robinson also warned financial services providers not to be complacent in the way that they approach employee fraud risk, or any other fraud risk. “Our review found that firms place greater emphasis on vetting staff in senior positions, as you might expect due to the trust placed on them,” said Robinson. “However, studies show that the recorded instances of lower level employee fraud are greater in terms of volume and size. This suggests that companies should ensure that suitably designed internal controls to prevent and detect fraud at lower levels within the organisation are in place,” he added.

Motivation

The motivation for employee fraud is two-fold – it can be for personal and professional reasons. PwC’s Clark says that “there is a growing temptation for employees – from the top of the organisation right through to the bottom – to commit fraud at work, either to ‘help’ the company by massaging its financial results, burying bad news, or choosing not to disclose some risks that might have an adverse effect on the business or their own position, or for personal gain to help pay debts, or to take what they feel is ‘owed’ to them.”

“Either way, there is a real need for financial services firms to ensure that they have adequate fraud controls and procedures in place throughout the organisation, so that everyone is clear about what constitutes ‘fraud’, how incidents or suspicions can be reported, and how frauds may be uncovered, and ideally, prevented. To

For your consideration...

The FSA has outlined a number of key risks that it believes financial services providers should consider as part of their revised risk assessments:

1 Understanding the organisation’s risk profile

Analysis of an institution’s threat profile needs to include the identification of fraud threats specific to the products and services provided and, additionally of general factors which make the institution more susceptible to fraud.

2 Organisational change

Change often introduces uncertainty and temporary destabilisation, which can affect levels of risk.

3 Employee’s experience and knowledge

Stable, experienced employees can generally contain risk levels, while regular or major employee changes can have an impact on levels of motivation.

4 Changes to the product range

The fraud risk of long established products will generally be well-known while new or changed products bring increased levels of fraud risk.

5 Systems changes

Changes to IT systems, and indeed to manual procedures, can unwittingly introduce additional fraud risk.

6 Level of fraud-averse culture

An organisation without a fraud-averse culture is likely to have higher levels of fraud risk.

7 Changing risks to the organisation

Firms should continue to analyse the changed risks of the new environment and avoid the temptation to cut back on operational risk management, especially financial crime risk management. Some examples are:

- Do authentication and approval procedures remain robust after you have downsized?
- Are you carrying out staff vetting when you move displaced staff into sensitive positions?
- Is increased use of temporary staff a source of infiltration risk?
- Is access to sensitive customer data on a need to know basis?

Source: *BBA Fraud Managers reference guide Chapter 1 (section 1.4.2.3)*

achieve this, functions like internal audit and human resources need to get together and share resources to help identify areas where these risks are most likely to occur,” he says.

Brett Feldon, EMEA general manager at speech and recognition software provider VeCommerce, says that “as the FSA implies, not only does a strategy need to encapsulate organised crime, it also needs to look more closely at the possibility of fraud closer to home”.

“Finding ways in which to address employee fraud is critical, especially in contact centre environments »

“The recorded instances of lower level employee fraud are greater in terms of volume and size”

» where there is often a high churn rate of staff that have daily access to sensitive information,” says Feldon. “Organisations need to look at how they can either improve their initial vetting process (which still isn’t a guarantee of preventing fraud) or investigate alternative ways of completely excluding access to private data,” he says.

The FSA has highlighted since April 2008 that poor data protection is a potentially massive fraud risk for many firms. Robinson believes that in today’s climate, criminals will know that members of staff may be more vulnerable to corruption. “Professional gangs are relentless in their efforts to exploit the weak links in the chain... they can get their hands on your customer’s personal details. Worryingly, we know from studies that UK bank account details are the most advertised ‘product’ on black market internet forums used to trade compromised data.”

Warning

But experts also warn of the dangers of mis-using customers’ personal information to boost sales. They point to the risk of commission-led sales teams ignoring best practice and internal guidelines to pitch “inappropriate” products and services to customers in order to secure bonuses.

Stephen Gregory, global financial services internal audit leader at Ernst & Young, says that “for some time, the FSA has stressed the importance of protecting customer’s data but it has still managed to flag up several incidences of where financial services providers have failed to live up to expectations. The FSA has already imposed massive penalties on firms for their mis-handling of customer data to push sales, such as in the cases of payment protection insurance (PPI), and this may be set to continue if bank staff ignore these rules and procedures to push sales to earn commission fees, or if

the organisation fails to understand the risks and address them.”

The regulator’s review of firms’ practices shows that poor information security controls represent a serious, widespread and high-impact risk. “We’ve warned that this risk continues to increase, so it’s disappointing that many firms continue to underestimate the risk of data loss and identity fraud to their businesses and customers,” said Robinson. “One of the key problems we found with some of the larger firms was not the level of resources applied to tackling the problem; rather it was the lack of co-ordination among relevant business areas. There is too much focus on IT controls and too little on office procedures, staff recruitment and vetting, monitoring and due diligence of third parties.”

Simon Morris, research and development director at risk management consultancy Pentura, agrees that “technology can really only be used effectively if there are solid business processes underwriting these”. Unfortunately, he adds, “businesses have a tendency to use technology as a point solution and derive a policy at a later date. The net result is poor business practices and exposure to exploitation.”

Over reliance

Clark also agrees that banks and insurers are relying too heavily on IT in the fight against fraud. “An IT system is only as good as its programming,” he says. “The system may not recognise all the potential risk issues that someone with some years of experience of working in that environment will immediately think of. Therefore, it is very important that management receives information from other sources – namely employees – so that it can get a better appreciation of all the risks and controls that need to be put in place to mitigate them.”

To combat incidences of fraud, the FSA is appealing for more firms

to share information with other providers, pointing to the latest CIFAS annual report as a measure of success. The fraud prevention service reports that its member organisations avoided losses totalling almost £1bn in 2007. Since 1990 the total figure is said to be £5bn. According to Robinson at the FSA, “this is a commendable example of industry-led solutions delivering real and tangible benefits”.

But he maintains that much greater co-operation is crucial if fraud is to be avoided and consumer protection properly maintained. “Why are over 180 CIFAS members not using and contributing to its staff fraud database? Surely in times where internal fraud is likely to be on the increase and with 130 CIFAS members already contributing there must be a good reason why these 180 firms are not using it, especially as I am told that it is included in their CIFAS membership fees. Perhaps they have another source to carry out their own equivalent due diligence on new staff?”

However, such hopes of co-operation may be naive. Clark says that it will be some time before financial services firms freely share their experiences of fraud with their competitors. “Recent trends have shown that banking frauds are becoming much larger in scale and that they demonstrate clear issues about poor internal control, so it is always doubtful that any bank is going to reveal too much for the sake of helping a rival,” he says. ●

“Experts also warn of the dangers of mis-using customers’ personal information to boost sales”