



THE FINANCIAL CRISIS AND EMPLOYEE FRAUD

Security Briefing

May 2009

Fraud On The Rise As Economy Slows

Greater workplace and financial pressures are making fraud an increasingly common problem during the global financial crisis. The Australian Consumer Fraud Taskforce has warned that consumer fraud is set to increase dramatically in Australia in 2009¹ while the operational impact of workplace fraud will be significant with rising levels of employee fraud, recruitment fraud and intellectual property theft. However, the economic downturn will also make fraudulent activities more difficult to maintain as organisations look more closely at their operations in the tighter financial climate. As such, the financial crisis is likely to lead to the collapse of fraudulent investment schemes and many high-profile fraud prosecutions.

The current high levels of fraud have been caused by a number of factors². Large scale corporate global expansion and the growing complexity of organisations have made it easier for fraud to go unnoticed, while technological advances (including the increased speed of computerisation and communication) and an increasingly transient workforce have increased the ease and frequency with which fraud occurs. However, fraud in such an environment is not inevitable - the proliferation of fraudulent activities today can largely be attributed to weaknesses in organisational security, including ineffective anti-fraud controls, understaffing of internal audit functions and a lack of commitment in enforcing anti-fraud mechanisms. With employee fraud levels rising, it is more important than ever that organisations have secure and robust internal controls and risk management systems. The organisations that fared best following the 1992 recession were those that switched their resources from front-end application processing into fraud and collections teams³. Businesses should thus expand their teams working on fraud prevention and detection to prevent excess losses and be in a strong position for the economic recovery.

**INTERNATIONAL OPERATIONS
GROUP PTY LTD**
Security Strategists

OFFICE

199 Gloucester Street
The Rocks NSW 2000
AUSTRALIA

POST

PO Box N260
Grosvenor Place NSW 1220
AUSTRALIA

PHONE

+61 2 8003 3933

EMAIL

2009@interopsgroup.com

WEB

www.interopsgroup.com

Workplace Fraud

High degrees of employee mobility and technological advances have provided ripe conditions for fraud in the current workplace environment. Employee fraud causes massive reputational damage to organisations, whatever field they are functioning in. At the start of the credit crunch in 2007, the Deloitte Global Security Survey found that 91 percent of employers were concerned about employee security weaknesses⁴. Employer fears over internal fraud are justified with many surveys carried out in recent years showing that the majority of fraudsters are employees, with over half being in managerial positions⁵. KPMG's Annual fraud barometer found that fraud by individuals had tripled in the UK from 2007 to 2008⁶ and a current global fraud survey reports that 85 percent of fraud is committed by employees⁷.

Employee fraud continues to be a problem in Australia with too few organisations enforcing comprehensive fraud monitoring and detection programs. Furthermore, a significant degree of workplace fraud that is detected remains unreported. A 2004 Deloitte survey found that 74 percent of Australian risk managers and investigators believed that less than a quarter of all fraudulent acts were being detected, while 41 percent believed that under 10 percent of fraudulent acts were detected⁸.

Common types of employee fraud include the manipulation, misuse or theft of data, payroll and expense fraud, misappropriation of funds, falsification of documents and financials, and intellectual property theft. Identity fraud has become an increasing risk, with financial institutions targeted in particular. Intellectual property (IP) theft has also become a major problem and is likely to increase with decreasing job security levels around the world. The likelihood of customer lists, software coding and business plans being transferred to the competition is rising.

The current financial crisis is placing increased pressure on employees to commit workplace fraud with more unattainable sales targets and a reduction in bonuses in the financial sectors. Employee fraud can sometimes be purely for personal financial gain; however it can also be connected to organised criminal networks. When an individual's economic circumstances are at risk, they are far more likely to act in ways they would have previously deemed to be unacceptable. Once workplace theft has begun to occur, it will tend to escalate.

KPMG Australia identifies gambling, greed and identity fraud as the main contributing factors towards a doubling of reported corporate fraud levels between 2006 and 2008. Gary Gill, head of KPMG Forensic Australia, has identified the typical fraudster as a 38-year old non-management male who has held his current position for four years by the time of detection⁹.

Donald Cressey, the 1950s criminologist, established what is now widely known as the 'fraud triangle'. Cressey hypothesised that three key elements

are necessary for an individual to turn to fraud: opportunity, incentive/pressure (or motivation) and rationalisation. During the current financial crisis all three elements of the triangle are increasing dramatically:

Opportunity

- ▶ Segregation of duties is a key part of fraud control and there will be less scope for segregation with fewer people employed. Cuts to the numbers of back office staff will reduce organisational capacity to conduct adequate recruitment screening to guard against job application fraud.
- ▶ Cost-saving measures, including security and fraud risk management budget cuts, will create gaps in control systems, thus leading to increasing opportunities for fraud to occur.
- ▶ Criminal organisations are becoming increasingly successful in obtaining confidential data such as bank account details. Such organisations will view the financial crisis as an opportunity rather than a threat, due to an increase in the number of employees offering to sell confidential or sensitive information as job security becomes threatened and mass redundancies occur.

Incentive/Pressure (Motivation)

- ▶ Increased financial pressures (both at home and in the workplace) will contribute to the motivation to commit fraud.
- ▶ Due to mass redundancies, those still employed will feel increasingly threatened and under pressure to commit fraud to aid their own financial or job security prospects.
- ▶ Job application fraud (including the withholding of criminal convictions and the provision of false references and qualifications) will rise with people becoming increasingly desperate to find jobs.

Rationalisation

- ▶ The worsening economic conditions will increase the rationalisation for committing fraud as more employees become disgruntled and morale dips due to lower-than-expected pay.
- ▶ Workers may persuade themselves that they have not received their deserved bonus, and are thus entitled to extra money gained through fraudulent workplace activities.

The Costs Of Fraud

It has been estimated that the annual cost to the Australian economy of financial crime stands at around \$5.88 billion. This figure represents nearly a third of the overall cost of crime in Australia and is only the direct cost of fraud. When taking into account indirect costs resulting from fraud, including investigation and prosecution, Deloitte Forensic has estimated that the cost of fraud to the Australian economy could be as much as \$10 billion a year¹⁰.

The Association of Certified Fraud Examiners estimates that losses incurred through fraud run at 7 percent of revenue for organisations in the United States¹¹. Likewise, the fifth annual UK Online Fraud Report estimated that one in eight businesses in 2008 suffered fraud losses in excess of 5 percent of total online revenues¹². The report also found that 40 percent of online merchants saw their fraud loss rate increase in 2008. These figures appear to be high but it is likely that many companies will be incurring fraud losses at more than these levels.

There are numerous costs associated with fraud in terms of time, money, productivity, reputation and customer relationships. While management and staff carry out post-fraud recovery processes (including dissecting the fraud, reconstructing records and generally repairing the damage done), they are drawn away from their regular duties and operations¹³. Due to the potential for the costs of fraud to escalate quickly, it is of utmost importance to invest in mechanisms that prevent fraud occurring in the first place.

Fraud reaches 13 year high in the United Kingdom

Fraudulent activity in the United Kingdom (UK) has reached a 13-year high with more than £1.1 billion (\$1.58 billion) coming into the country's courts in 2008¹⁴. KPMG's 2008 Fraud Barometer showed that financial services were the worst hit sector. The corporate sector was also badly hit with a five-fold increase in corporate fraud from 2007 to 2008. Cases of accounting fraud increased from a value of £22 million (\$31.6 million) in 2007 to over £145 million (\$208 million) in 2008. Fraud threats grew both internally and externally across all types of organisations (corporate, financial and public sector). Despite these figures, the majority of fraud committed since the credit crunch began in August 2007 is yet to come into the public courts.

Organisational Security

It is difficult to apply accurate figures to the losses a corporation did not suffer due to the presence of effective security controls and, as such, few organisations fully understand how much fraud is actually costing their business. Fraud will occur when there are weaknesses or gaps in control

systems, which result from inadequate fraud risk management programs and security funding cutbacks.

Most organisations do not have a comprehensive understanding of the fraud risks across all their business areas, and a large number have inadequate controls to address fraud risks¹⁵. Findings from the latest Ernst & Young annual global fraud survey show that 72 percent of companies surveyed did not provide anti-fraud policy training to their employees while 42 percent did not have a formal anti-fraud policy¹⁶. The costs associated with installing effective anti-fraud programs and investigating fraud are often a deterrent for companies.

When finances become tighter, organisations sometimes downsize the budget available for corporate security. However, as the economy slows down, security should be of utmost importance. Both the governmental and private sectors will be more susceptible to industrial espionage and fraud due to security cutbacks and increased focus on other security sectors (such as terrorism). The cutting of security budgets will lead to a lack of adequate controls and thus an increase in losses through fraudulent activities. Security infrastructure shortcuts do not save organisations money in the long term as effective fraud risk management programs will offer far higher savings (through the prevention of potential losses) than the costs involved in their set up and maintenance.

International Operations Group

Recommendations

Review current internal fraud procedures

A review must be undertaken to thoroughly understand an organisation's current internal fraud procedures and assess what further steps are required to help ensure a comprehensive anti-fraud program. The vast majority of organisations need to update their existing fraud risk assessment, monitoring, control, detection, and reporting processes.

Conduct a risk assessment

As fraud risks will be unique for each department and line of business, there is no standard formula for an anti-fraud program. A comprehensive risk assessment must be undertaken to define the specific risks of employee fraud in each business area and across the whole organisation. Identified risks should then be prioritised according to their severity so that suitable mitigation controls can be established. How critical a risk is deemed to be will depend on its potential consequences and the likelihood of it occurring. Fraud risk

assessments should be repeated regularly to ensure their continuing validity and effectiveness.

Implement fraud-monitoring mechanisms

A reliable whistle-blowing system must be implemented in all business areas to allow the anonymous reporting of suspected employee fraud. Anonymous whistle-blowing systems are one of the most effective tools in detecting, preventing and deterring workplace fraud. It has been estimated that more than half of internal frauds are detected by a colleague¹⁷. In the current economic environment, staff should monitor changes in colleagues' work habits and patterns (i.e. staff working late when they would otherwise not do so). Although a number of organisations have effective audit functions, these are not necessarily at the level where fraud may occur. Front-line operations and finance personnel are vital first and second levels of defence against the occurrence of fraud¹⁸. Management oversight and internal audits are crucial in ensuring that fraud-monitoring mechanisms are being adhered to.

Implement detection and control procedures

Appropriate risk mitigation controls must be in place to treat workplace fraud risks. The level of control will be dependent on the prioritisation of risks established during the risk assessment. Fraud detection tests (including data analytics) should be developed to routinely check databases and financial figures. A workplace culture that encourages openness and reporting is necessary to ensure that suspicions of employee fraud (whether reported by directors, auditors or low-level staff) are comprehensively followed up and dealt with. The frequency of workplace fraud can be minimised by ensuring that recruitment checks are comprehensive (including checking an applicant's identity, credit background, previous employment, qualifications and references). Response to suspected workplace fraud must be prompt and involve thorough, independent investigations with lessons learned applied across an organisation's entire anti-fraud program.

Fraud awareness training should be given to staff involved in key operations in high-risk business areas. Such training will enable effective implementation of fraud risk management processes and will help in the future identification of emerging risks.

It is vital that the separate elements of fraud monitoring and fraud detection are coordinated across the whole range of a business's activities. An organisation's gatekeeper functions (loss prevention teams, in-house legal, security, and internal audit and compliance functions) must work together for an effective workplace fraud risk management strategy to be implemented¹⁹.

Adopting an anti-fraud stance at the organisational level

There must be effective management oversight to ensure that the anti-fraud processes are being implemented and that an anti-fraud culture is developed.

Anti-fraud plans and policies must be promoted and enforced across the business. The clear communication of a formal, written fraud policy will ensure that employees understand the organisation's attitude towards fraud. The Australian Auditing Standard AUS210 places the responsibility for the prevention and detection of fraud with an organisation's management²⁰. However, it should not only be a legal obligation for managers to commit to anti-fraud programs. Adopting an anti-fraud ethic across a whole organisation is vital in ensuring the success of an anti-fraud program.

Dr. John Demartini, a world leading human behavioural expert, advises that leaders need to inspire their workforce to ensure that the correct values filter through the whole organisation. Demartini states that fulfilled and inspired employees will be dedicated to the ethics and processes of an organisation. As such, if employees' core values associate with anti-fraud ethics, then anti-fraud processes will be effective. In these harsh economic times, it is more important than ever for leaders to increase motivation levels and promote anti-fraud values within their workforces. In such a way, anti-fraud values, tools and processes need to be actively embraced by the leaders of an organisation for employees to follow suit. Thus, the establishment of a comprehensive anti-fraud program and stance from the top down will maximise the probability that anti-fraud ethics and processes will be adopted throughout an organisation's workforce.

Continuous monitoring, evaluation and review of program

The risks associated with fraud will continually change and, as such, risk management programs need to be continually assessed and updated to ensure that they remain comprehensive. Once an anti-fraud system has been installed, it must be regularly reviewed and maintained to ensure that it remains effective. Regular assessments will ensure that gaps and vulnerabilities are minimised and fraud risk management strategies continue to be effective with regard to prevention, monitoring, detection and response.

International Operations Group - Services

International Operations Group offers a range of investigation and security consulting services to assist companies or individuals manage incidents of fraud. Our investigators are experienced fraud detection, fraud recovery and fraud risk management specialists.

We provide critical-response support and advice relating to incidents of fraud, helping to contain and recover losses once fraud is detected. Our team works with clients to prepare and instigate fraud response and fraud risk management plans.

We also place a strong emphasis on assisting clients prepare fraud prevention strategies and associated policies.

International Operations Group's Senior Investigators are able to provide investigation support relating to numerous types of fraud, including, but not limited to the following:

- Embezzlement,
- Financial statement fraud,
- Insurance fraud,
- Investment fraud,
- Bribery and corruption,
- Misappropriation of funds,
- Phantom vendors,
- Stock loss / theft,
- Procurement fraud, and
- Mortgage fraud.

Our consultants are experienced in the provision of fraud-related litigation support and in the preparation of detailed 'Briefs of Evidence' in both civil and criminal matters.

Furthermore, we have a team of surveillance operatives, general investigators and security consultants, all of whom are able to provide advice and support on a wide-range of issues, offering a holistic approach to security and fraud prevention and response.

Please email us at 2009@interopsgroup.com or telephone us on +61 2 8003 3933 for additional information or for fraud investigation response and/or fraud risk management support.

For more information on our fee-based intelligence updates or bespoke reporting, please email Rob Stevenson - rob@interopsgroup.com. Rob can also be telephoned on +61 [0] 420 244 909.

¹ Australian Competition & Consumer Commission (2009), 'Scams proliferate in global financial crisis', <http://www.accc.gov.au/content/index.phtml/itemId/862364/fromItemId/142> [accessed 20 April 2009]

² Ernst & Young, 'Corporate Fraud – Why fraud happens', http://www.ey.com/global/content.nsf/China_E/Corporate_Fraud [accessed 20 April 2009]

³ Credit Industry Fraud Avoidance System (2009), '2008 Fraud Trends – Fraud on the increase', http://www.cifas.org.uk/default.asp?edit_id=896-57 [accessed 20 April 2009]

⁴ Deloitte (2007), '2007 Global Security Survey', http://www.deloitte.com/dtt/research/0_1002.sid=1013&cid=170582_00.html [accessed 20 April 2009]

⁵ Ernst & Young, 'Corporate Fraud – Why fraud happens', http://www.ey.com/global/content.nsf/China_E/Corporate_Fraud [accessed 20 April 2009]

- ⁶ KPMG UK (2009), 'Fraud nears record levels in 2008 – and worse to come, says KPMG', <http://www.kpmg.co.uk/news/detail.cfm?pr=3334> [accessed 20 April 2009]
- ⁷ Spencer, V., 2 March 2009, 'Companies face heightened risk of fraud in current global credit crisis', <http://energy.pressandjournal.co.uk/Article.aspx/1086429?UserKey=> [accessed 20 April 2009]
- ⁸ Deloitte Forensic (2004), 'Corporate fraud on the rise, Deloitte survey reveals', http://www.deloitte.com/dtt/press_release/0.1014.sid%253D5527%2526cid%253D60713.00.html [accessed 20 April 2009]
- ⁹ KPMG Australia (2009), 'Unmasking the face of corporate fraud', <http://www.kpmg.com.au/Default.aspx?tabid=214&kpmgarticleitemid=3533&frompress=true> [accessed 20 April 2009]
- ¹⁰ O'Toole, F., Deloitte Forensic (2006), 'The real cost of fraud', http://www.deloitte.com/dtt/cda/doc/content/016382_Web_article2_The_Real.pdf [accessed 20 April 2009]
- ¹¹ Association of Certified Fraud Examiners '2008 Report to the Nation on Occupational Fraud and Abuse', <http://www.acfe.com/resources/publications.asp?copy=rttn> [accessed 20 April 2009]
- ¹² Cybersource (2009), 'UK Online Fraud Report 2009', Cybersource, http://www.cybersource.co.uk/resources/fraud_report_2009.php [accessed 20 April 2009]
- ¹³ Coenen, T. (2008), 'The True Cost of Fraud: Indirect Costs', <http://www.allbusiness.com/crime-law-enforcement-corrections/criminal-offenses-fraud/5222152-1.html> [accessed 20 April 2009]
- ¹⁴ KPMG UK (2009), 'Fraud nears record levels in 2008 – and worse to come, says KPMG', <http://www.kpmg.co.uk/news/detail.cfm?pr=3334> [accessed 20 April 2009]
- ¹⁵ PricewaterhouseCoopers UK (2009), 'Fraud in a Downturn – A review of how fraud and other integrity risks will affect business in 2009', http://www.pwc.co.uk/eng/publications/fraud_in_a_downturn.html [accessed 20 April 2009]
- ¹⁶ Spencer, V., 2 March 2009, 'Companies face heightened risk of fraud in current global credit crisis', <http://energy.pressandjournal.co.uk/Article.aspx/1086429?UserKey=> [accessed 20 April 2009]
- ¹⁷ O'Toole, F., Deloitte Forensic (2006), 'The real cost of fraud', http://www.deloitte.com/dtt/cda/doc/content/016382_Web_article2_The_Real.pdf [accessed 20 April 2009]
- ¹⁸ PricewaterhouseCoopers UK (2009), 'Fraud in a Downturn – A review of how fraud and other integrity risks will affect business in 2009', http://www.pwc.co.uk/eng/publications/fraud_in_a_downturn.html [accessed 20 April 2009]
- ¹⁹ PricewaterhouseCoopers UK (2009), 'Fraud in a Downturn – A review of how fraud and other integrity risks will affect business in 2009', http://www.pwc.co.uk/eng/publications/fraud_in_a_downturn.html [accessed 20 April 2009]
- ²⁰ Australian Accounting Research Foundation (2004), 'AUS210: The Auditor's Responsibility to Consider Fraud in an Audit of a Financial Report', <http://www.auasb.gov.au/admin/file/content102/c3/AUS210.pdf> [accessed 20 April 2009]