



forensics @ ferriers

Uncovering the facts with the Ferrier Hodgson Forensics team

Fraud in the workplace: **she did it!**

When the topic of employee fraud or theft is mentioned, do you automatically imagine the perpetrator is a middle-aged male white collar worker? You wouldn't be alone.

Indeed, results published in the Association of Certified Fraud Examiners (ACFE) 2006 Report to the Nation on Occupational Fraud and Abuse found that more than 60 per cent of frauds were committed by men, mostly aged from 31–50, and mostly long-term employees (64 per cent were committed by employees with five or more years of service).

But a spate of recent fraud cases investigated by Ferrier Hodgson seem to differ from that in one key respect: they were all committed by women. Fraud appears to be a disturbing new pastime for middle-aged women with previously unblemished employment records.

Looking at the details of the investigations, there were two common threads: firstly, a number of the women admitted to a gambling addiction; secondly, all of the organisations in question had poor internal financial controls and procedures, which the women took advantage of.

There is a clear lesson to be learned by organisations relying on antiquated financial procedures created for a different era.



Cash Fraud

Ferrier Hodgson was approached by the board of a medical facility provider to investigate a female receptionist who was responsible for accepting payments from in-patients. Her job was to enter the payments into the accounting software and issue receipts.

However, our investigation revealed the receptionist had been accepting cash payments from the patients, entering them into the accounting software but later reversing the payments and recording them as credit card transactions. At the end of the day when cash reconciliations were done, the cash balances in the till reconciled to the expected cash recorded in the accounting software.

During our investigation we learned that on one occasion the receptionist actually drove a patient to a nearby ATM machine for him to withdraw the cash to pay for his treatment. The receptionist then misappropriated the cash.



It was estimated that the receptionist had stolen approximately \$300,000 from the organisation, but given the poor accounting records, only a small portion of the misappropriated funds could be directly linked to the receptionist.

This ties in directly with the ACFE report, which suggests that of all asset misappropriation frauds, 87.7% involved the misappropriation of cash.

Cheque Fraud

Another case Ferrier Hodgson has reviewed involved a bookkeeper – employed for 13 years by a wholesale business – who misappropriated approximately \$1.6 million.

The bookkeeper prepared company cheques to any one of five financial institutions which the organisation dealt with on a regular basis. The bookkeeper had a personal account with each of the five financial institutions.

The directors of the organisation signed the cheques payable to the financial institutions believing they were for work-related issues. Whilst the cheques were not made personally payable to the bookkeeper, each of the five financial institutions banked the cheques into her personal account.

The fraud was detected when a director began querying the cashflow difficulties the organisation was facing. The employee, who admitted to a gambling addiction, was convicted and sentenced to six years jail.

This, too, is supported by the ACFE survey, which reported that cheque tampering accounts for 17% of all cash misappropriation cases.

How to foil fraud

Switched-on finance and accounting executives know where the risks of fraud lie, so why do simple control failures continue to be such a significant contributor to corporate fraud? Implementing effective controls can be straightforward. Here are some hypothetical examples and ideas for controlling the environment and curbing fraud.

1. An employee arranges for an entity controlled by her husband to be included on the authorised suppliers list. Subsequently, a number of ‘creditor’ payments are made which, in effect, find their way into the hands of the employee.
 - Ensure only specified directors can authorise new suppliers. Consider using dual signatories, and the use of credit checks and/or company searches on the supplier. Consider cross-matching to employee or HR data to determine whether the supplier entity or its owners have any connection with employees. Consider analysing payroll and supplier data for multiple bank account details.
 - Segregate roles - ensure employees involved in supplier set up are not involved in supplier payments.
 - Ensure a senior executive or Director authorises all payments, whether by cheque or EFT.
 - Two employees (from different business areas) should perform electronic banking functions together (ie: one employee, usually from the finance department, has the user name, and the other employee, usually a senior manager, has the password).
 - Undertake ad-hoc or surprise data matching. For example, try to cross-match employee bank account details (bank, branch or account numbers) to those of suppliers.
 - Consider data analysis aimed at identifying non-conforming transactions or transaction patterns. Several methodologies and tools are available.
 - Make use of a confidential whistleblowing service and follow up all information – research shows that fraudsters’ activities or behaviour patterns are often common knowledge in the organisation.



2. An employee in charge of warehousing diverts incoming shipments of inventory for personal use. Many of the controls suggested above are also appropriate here, but in addition:
 - Ensure the employee who orders inventory is not responsible for accepting delivery of the inventory.
 - Ensure all delivery dockets are authorised by the appropriate personnel prior to payment of invoices.
 - Review adequacy of control over physical access to the warehouse by employees, suppliers and vehicles. Review access and consider whether the identity of all visitors can be verified. Is there a need for greater physical security over certain categories of inventory which are more susceptible to theft?

3. An employee is able to access elements of sensitive design specifications which are a key intellectual property asset of the company. This valuable intellectual property ends up in the hands of a competitor.
 - Be aware that employee fraud does not always involve the theft of physical property – as detailed in Issue 11 of *Forensics@Ferriers*, theft of intellectual property by employees is a hot issue. Recent media coverage highlighted a former Coca-Cola secretary who was sentenced to eight years jail after she plotted to sell company secrets about new Coca-Cola products to PepsiCo for \$US 1.5 million. What controls do you have in place to combat IP theft or misuse?
 - Undertake surprise reviews of IT security, such as ‘penetration testing’ targeted at finding evidence of access to the key IP assets.
 - Consider physical security and the ease with which employees can copy and remove data from company networks. In extreme cases, some organisations have prohibited the use of USB drives in an attempt to stem the flow of IP loss.

In our experience, good controls should be (but often are not) about ensuring an element of surprise, listening to the concerns of employees, investing in resources to ensure controls are continually reviewed and tested, and thoroughly following up all anomalies which come to light.

Expenses Fraud

Ferrier Hodgson recently investigated the CEO of a charity who misappropriated approximately \$500,000 over a 12-month period via the misuse of credit cards and petty cash. The CEO used the charity funds for personal expenses.

This CEO must have been a particularly well-groomed woman. Her credit card transactions revealed she regularly visited her hair salon three times a week.

The ACFE study attributes 19.5% of cash misappropriation cases to fraudulent claiming of expenses.

Funds Transfer Fraud

A bookkeeper employed for ten years by a financial planning firm misappropriated approximately \$1 million.

The bookkeeper had authorised access to the organisation’s electronic banking facilities and regularly transferred funds to her personal account.

Additionally, she drew cheques payable to places such as Officeworks, had them authorised and signed on the premise that the funds were being used to purchase office equipment and assets. She would then purchase the goods for her personal use or sale.

The fraud was detected when her organisation decided to perform an audit of its asset register and realised there was a large number of pieces of office equipment that had been purchased that could not be located in the office. This employee also suffered a gambling addiction.

The ACFE survey reported that electronic banking transfers accounted for 6.5% of cash misappropriation cases.



Internal Controls

In each of these examples, the employees were able to misappropriate cash from their various employers due to a severe lack of internal controls and procedures surrounding the handling of cash, recording of cash, payments of expenses via cheques and via electronic banking. Especially today, when organisations routinely make use of technology such as accounting software, point-of-sale systems and electronic banking, organisations need to ensure their internal controls are constantly revised and amended to combat the potential frauds that can occur.

In relation to our recent investigations, the establishment of and compliance with internal controls could have assisted in the prevention of the frauds (see call-out box).

Ferrier Hodgson's experience in relation to fraud investigations has shown us that fraud takes on many shapes and forms – in terms of the profile of the perpetrator, the organisation the fraud occurs in and the nature and size of the fraud.

Organisations need to be vigilant to protect themselves against fraud, not only by ensuring they have strong internal controls implemented, but also through assurance that their internal control procedures are adhered to and maintained.



Melinda Bowman
Senior Manager, Melbourne
phone: +61 3 9604 5650
email: melinda.bowman@fh.com.au

For more information about our Forensic Services please contact:

Sydney: John Temple-Cole
+61 2 9286 9919
john.temple-cole@fh.com.au
Andrew Ross
+61 2 9286 9906
andrew.ross@fh.com.au

Melbourne: Greg Meredith
+61 3 9600 4922
greg.meredith@fh.com.au

Brisbane: Tim Michael
+61 7 3834 9228
tmichael@qld.fh.com.au

Adelaide: Peter Holmes
+61 8 8100 7663
pholmes@sa.fh.com.au

Perth: Garry Trevor
+61 8 9221 2460
gtrevor@perth.fh.com.au

New Zealand: Grant Graham
+64 9 307 7865
grant.graham@ferriers.co.nz

Hong Kong/China: John Tudorovic
+852 2820 5610
jtudorovic@fh.com.hk

Singapore: Tim Reid
+65 6416 1400
timr@fh.com.sg

Or find out more about Forensics at:
www.ferrierhodgson.com

[Related newsletters and articles](#) >

If you have any questions or comments about Forensics@Ferriers please email [Ferrier Hodgson](mailto:Ferrier.Hodgson)

[Subscribe](#) > [Unsubscribe](#) > [Disclaimer](#) > © Ferrier Hodgson 2007

FORENSIC ACCOUNTING

FINANCIAL INVESTIGATIONS & FRAUD

BUSINESS VALUATION

FORENSIC IT



FERRIER HODGSON
FORENSICS