PRICEWATERHOUSECOOPERS

Corporate Fraud:
Prevention, Detection and Investigation

fas/3103

A practical guide to dealing with corporate fraud

TABLE OF CONTENTS

1 INTRODUCTION

Corporate fraud is an undeniable fact of business life, affecting businesses large and small. New technologies such as the Internet, and the development of fully automated accounting systems, have increased the opportunities for fraud to be committed. Once suspected or discovered, investigating fraud is a specialist task requiring experience and technical skill. There is no doubt that fraud is best prevented, rather than dealt with after the fact.

Unfortunately, there is no foolproof method of preventing fraud, although there are a range of fraud prevention techniques which been proven to be successful. Other techniques may be used to pro-actively test for fraud profiles, and to further investigate so that fraud incidents are satisfactorily resolved.

The most effective and appropriate response to the problem of fraud involves a combination of fraud prevention, detection and investigation techniques. This paper will provide a basic summary of these techniques, which from a “best practice” perspective should be implemented in organisations.

2 FRAUD RISK ANALYSIS

Few competent managers would doubt that fraud is a significant potential problem for their organisations. Newspapers are full of reports, editorials and surveys which suggest fraud is commonplace, easy to commit and unlikely to be detected. The cost of fraud to Australian business is difficult to quantify, but according to the Australian Institute of Crime, it may be as high as A$14 Billion annually.

Identifying high fraud risk areas in an organisation is the first step in dealing with the problem of fraud. These risk areas can vary from industry to industry and company to company.

Some of the more common risk areas are outlined below:

- ***Accounts Payable*** — Purchasing and expense-related fraud is probably the most common fraud encountered, and is likely to affect the majority of small to medium sized businesses at some stage. The opportunities for fraud in purchasing are high, as this is one of the main areas where funds "leave" a business. Fraudulent transactions can be easily concealed in these outwards flows, in the purchase if material and assets, and the payment of expenses. Automated detection tests, discussed later in this paper, can be applied to company records to identify purchasing "Fraud Profiles" requiring further investigation.
- ***Sales and Accounts Receivable*** — The most commonly encountered frauds here involve discounting and credit. Excessive discounting in return for "kickbacks" is relatively common (and a particular problem in agency dealings in Asia). Similarly, millions are lost from organisations through bad credit obtained fraudulently, often through the corruption of a sales or credit employee.
- ***Cash and Cheques*** — Control procedures are usually in place in regard to cash, yet they are often ignored where cheques are concerned. Cheque theft and resulting fraud, though usually on a "small" scale, is surprisingly commonplace. Larger scale frauds can occur where bank reconciliations are weak and separation of duties is not performed.
- ***Physical/Access Security*** — Physical controls over access to potentially sensitive areas such as cash management, inventory storage, and accounts payable are rarely as strong as they should be in many organisations. This can lead to large scale, organised fraud resulting from the theft of treasury payment instructions, passwords, sensitive corporate information and company assets.
- ***Corporate and Personnel Policies*** — Most company policies in respect of fraud control, confidentiality, information security, personnel screening, etc. remain inadequate when applied against the risks. Care should be taken that such policies are in place, publicised and enforced as a fraud prevention measure.
- ***Computer and Communications Security*** — In many companies, computer system vulnerability to external and internal unauthorised access, including hacking, theft of passwords and electronic eavesdropping, is high. The incidence of 'high tech' fraud attempts is increasing, and will continue to do so.

- ***Insurance Cover*** — Fraud and theft related insurance coverage should be evaluated and reviewed according to relevant risks. Fidelity insurance is notoriously difficult to claim against, yet it may be the only means of recovering funds lost through fraud.

Management should consider conducting a fraud risk analysis of their business, addressing fraud risks in all areas of operation. A typical fraud risk analysis will involve a physical inspection of important sites, detailed examination of company policies and procedures, interviews with key employees, and examination of accounting records, computer systems and corporate documentation.

3 FRAUD PREVENTION AND CONTROL TECHNIQUES

Fraud prevention is a topical issue, and corporate governance requirements in Australia have never been higher. Cost cutting and loss prevention have become important ingredients in modern corporate profit strategies, and increasing public awareness has forced public institutions to take a more thorough approach to managing the taxpayer dollar.

This environment has not stopped the fraudster; rather, he/she has been forced to change tactics and targets. The modern "professional" fraudster has become more sophisticated, developing schemes to manoeuvre around accounting controls. The "opportunist" fraudster, on the other hand, perhaps lacking the sophistication or the motivation to avoid improved controls and security, must choose his targets more carefully, selecting only those without effective controls and anti-fraud procedures. The challenge for modern organisations is to develop a combination of fraud control and security procedures which will thwart even the most determined and skilled professional fraudster; whilst at the same time discouraging the opportunist from considering any attempt.

The following summary outlines some basic fraud control and risk minimisation techniques.

Corporate Fraud and Security Policies

In any organisation staff can only be expected to comply with policy if it is clearly set out in a comprehensive document which details procedures to be followed.

Where no such policy document exists, it is often difficult to prove that employees or external parties have knowingly acted against the interests of the organisation. Indeed the lack of clear guidelines is often the first excuse which "offenders" will use - "I didn't see anything wrong in accepting a free holiday - nobody said it was against company rules" is an example of an actual defence forwarded by a buyer who received such a bribe from a vendor.

A comprehensive policy document should be prepared and made available to all employees, who should be asked to sign a declaration that they have read and understood the policy requirements. The document should spell out general policy in regard to:

- acceptance of gifts and entertaining
- conflicts of interest
- criminal and/or civil redress against personnel
- breaching the policy guidelines.

The policy document should also set out the consequences of fraudulent action and/or withholding information concerning any such action. It is also desirable that regulations relating to specific areas of the organisation's work should be set out for the benefit of staff working in these areas.

The document should make it clear it is the responsibility of staff to report any malpractice to management. In practice there is often a reluctance to do this as some staff interpret such action as "disloyal". Because of this an alternative method of reporting fraud, theft, waste and so on can be introduced and explained in the policy document. For example, fraud "Hotlines" have proved useful in the past as a means of encouraging the reporting of fraud incidents.

Payment Controls

Fraud in purchasing and procurement has seen an unprecedented increase in the last few years. Whatever the reasons behind this trend it is vital that organisations are adequately protected against this type of fraud which can result in substantial additional costs to the organisation.

Purchasing fraud frequently involves the payment of "kickbacks" or bribes, which are paid to decision makers within the purchasing organisation in exchange for the award of supply contracts. Fraudulent purchasing schemes can be sophisticated and difficult to detect. Such schemes can operate for years before they are discovered.

An important point to remember is that the payment of a kickback represents a cost to a supplier. In most cases, the supplier will seek to recover that cost, usually through undersupply, inferior product, or over invoicing. In nearly every case, the benefit to the supplier (and the cost to the purchaser) far outweighs the value of the kickback.

There are a number of ways in which an organisation can protect itself against procurement fraud. Practices recommended are as follows:

- pre-qualification of prospective vendors ("due diligence");
- ensure suppliers and staff are fully aware of company policies in regard to gifts and entertaining, and conflicts of interest;
- ensure proper levels of demand control to avoid unnecessary over-ordering of stocks, consumables and so on;
- establish clear purchasing authorisation levels;
- all invitations to tender on contracts should carry a declaration that the company is committed to the prevention of fraud, together with a Hotline number through which any prospective supplier or individual can report suspicions of fraud;
- copies of invitations to tender should be filed for future inspection to ensure that specifications are identical and that no company is given a more difficult specification to cause them not to bid or to submit a higher bid than it otherwise would;
- all contract documents should carry a right to audit clause which will facilitate an in-depth audit of the supplier's records should evidence of corruption come to light; and
- strict controls should be applied to supplier masterfile data including procedures to monitor dormant suppliers and to prevent illicit alterations to master file data.

It is also good practice to carry out periodic checks to ensure that invoices are from genuine companies, and not from shelf companies operating from "serviced office"

addresses or invoices printed simply to facilitate payment against non existent supplies of goods or services. Check of company ownership can be performed through the ASIC.

Sales and Inventory Controls

Sales and inventory frauds are often closely related. Such frauds will usually involve the following:

- Excessive discounting for the supply of goods and services;
- Theft of warehoused stock or diversion of stock in transit;
- Uninvoiced sales;
- Unauthorised award of credit notes; and
- Fraudulently obtained credit.

Strengthening controls in sales and inventory to prevent the frauds described above will usually involve a greater degree of enforcement of security standards, authorisation procedures, and "separation of duties" protocols.

Warehouses should always be maintained under strict security and surveillance; no stock should be permitted to leave a warehouse without appropriate checks that the stock ordered matches the stock being removed.

Credit notes should be awarded only after sign off by senior management unconnected with the sales process. Discounts should be monitored regularly using auditing programs, and discount levels should be set and maintained by non-sales management.

Sales and inventory controls would appear to be common sense, yet many frauds occur in this area because controls are ignored or not enforced. This is particularly the case in organisations with a strong "sales at any cost" culture.

Pre-Employment Screening

It is a well known fact that the majority of fraud is committed by employees. Pre-employment screening is therefore the first defence against fraud and yet it is only in the last few years that many organisations have come to appreciate its importance. This has culminated in the recent release of a draft Australian Standard on Pre-Employment Screening, "DR 99025 – Human resources management – Part 1: Pre-employment checking".

This change of thinking is a result of a combination of circumstances, such as publicity concerning organisations who have unwittingly employed criminals in high security or sensitive positions, and in many cases from personal experience involving candidates with false qualifications.

In recent years many cases have been publicised which adequately demonstrate that proper screening is not a luxury option. In these and other cases disaster could

have been averted if proper pre-employment screening had been carried out. It is a fact that the cost of proper screening is far outweighed by the cost of one bad recruit.

To reduce the risk of bad recruitment the organisation should have clearly defined standards which have to be satisfied. The first source of information is the candidate, therefore a comprehensive application form should be required to be completed by all applicants. Candidates should be told that it is the company's policy to carry out in-depth screening prior to their appointment, and should be asked to sign a release form or similar document which may be required during the screening process.

The application form (or failing that, the Curriculum Vitae) provides the basis for detailed checks to be carried out i.e. referees, educational qualifications, previous employers, public records and so on. The following should be undertaken as a matter of course:

- referees *and* past employers (preferably line managers) should be spoken to after their identities are independently confirmed. Bear in mind that referees provided by the candidate are hardly likely to provide unfavourable information on the candidate, even if they are aware of such information.
- all educational certificates should be inspected and independently verified. (Desk top publishing facilitates the production of most convincing documentation with little effort). Contact the institutions for verification of qualifications and professional memberships, rather than relying exclusively on candidate supplied certificates.
- carry out relevant background searches through on-line database systems. These might include directorship searches to ensure there are no potential conflicts of interest, bankruptcy searches, and media searches which might provide further information on the candidate's background.

Taken together, all of the above checks should assist you to build up an accurate picture of the candidate's experience, background and qualifications.

Pre-employment screening is a specialialist task requiring investigative skills and access to a wide array of public information databases. Many organisations, particularly those involved in financial services, prefer to outsource this work to screening experts. Further, it should be remembered that very few placement companies perform employment checks to the standard recommended in this article. For further information on PricewaterhouseCoopers Pre-employment screening service, please contact Guy Underwood on (02) 8266 7832.

4 PRO-ACTIVE FRAUD DETECTION

Most frauds are detected either by accident or by "tip-off". Organised, pro-active fraud detection is rare in most organisations. Most smaller organisations do not have an internal audit function, and the role of the external auditor does not include pro-active searching for fraud.

It is possible to discover evidence of fraud, even where there is no prior suspicion, although it is usually obscured within the millions of items of valid data held on computer files. Manual testing is rarely an effective or efficient solution, and hardly the job of time pressed management or external auditors. An automated fraud detection system is required which can search through millions of transactions and other data to identify those which might be worth a "closer look". This is particularly true of purchasing transactions.

A fraud detection program can be automated, and can provide management or the auditor with a detailed list of questionable transactions, suppliers and so on which can be further investigated..

Automated fraud detection will also complement a company's existing schedule of audit visits, making the best use of valuable and often scarce resources. It is a tool which will quickly identify problem areas and can also be used, where applicable, to audit the records of suppliers where a "right to audit" exists.

Automated fraud detection involves running an audit based software program on a company's invoicing and payment history, supplier and employee databases to quickly identify, for example:

Collusion Between Suppliers and Employees

Tests include:

- comparison between supplier and employee address and telephone/fax details
- analysis and comparison of supplier and employee banking details.
- duplicate employee or supplier addresses

Positive results from these tests might indicate that employees are also operating as suppliers, or that your suppliers are related to your employees. Such a result might indicate fraud and would probably indicate a conflict of interest.

Suppliers Fitting Known Fraud Profiles

Tests include:

- identification of suppliers with offshore bank accounts;
- false Australian Company Numbers ("ACN's");
- suppliers operating from accommodation addresses, or serviced offices.

Many purchasing related frauds involve false invoicing and the creation of fictitious corporate identities. It is common in more sophisticated frauds that this identity will include a "legitimate" postal address and telephone/ fax details, which are provided by serviced office companies across Australia. A database of these office details can be compared against supplier details to identify suppliers for further enquiry.

Questionable Transactions and Payments

Tests include:

- invoices for amounts just below authorisation levels ("Break Point Clustering");
- round value payments;
- early payments;
- high value, one off payments;
- duplicate invoice numbers and payments

and other dedicated programs can be run depending on the specific need.

Automated fraud detection testing is an efficient means of identifying potential fraud using commercially available audit software, and should be included as part of your organisation's overall response to fraud.

5 FRAUD INVESTIGATION — AN EFFECTIVE RESPONSE PLAN

It is important to remember that when fraud is first suspected the matter is likely to be more serious than it may initially appear. This is because fraudsters rarely restrict their activities to only one area, and therefore every effort should be made to obtain as much information as possible before anyone is challenged or confronted. This is particularly important in organisations, where the temptation to simply question an employee as soon as a suspicion is raised is strong due to the close working environment.

It is also important to be aware that larger scale frauds of the modern era are often international in nature. Therefore any contingency planning must include measures for taking legal and investigative action across jurisdictions.

Initial actions are crucial to the eventual outcome and, if a proper strategy is put in place and adhered to, then the extent of fraudulent activity can usually be assessed and action taken to resolve the matter successfully (this usually means assimilating sufficient evidence to dismiss errant staff and to take civil and/or criminal proceedings against those concerned in the fraud/s if so desired).

Conversely, the wrong actions at this early stage can lead to a botched investigation, destruction of evidence, financial loss and possibly, action against you and/or the company.

The following should be considered as a guide to the actions which should be considered in cases where suspicion arises:

Stage 1

- continue as normal, giving no indication that you are suspicious;
- initiate a covert investigation using internal investigators or external specialists. Together with the selected investigators, devise a strategy for the investigation (*see Stage 2 below*);
- list all reasons for suspicion;
- keep a detailed log of all actions and events from the moment of first suspicion onwards;

and only advise/involve those who *absolutely* need to know.

Stage 2

The investigation strategy may include:

- out of hours search of suspect's desk/office/work area;
- full background searches of suspect companies and individuals using public databases and so on;
- downloading and analysing the content of the suspect's office personal computer using specialist software (such as DIBS, or SAFEBACK) which will recover deleted or hidden files - very often these will contain documents of interest. Note that the obtaining of computer evidence, known as "Computer Forensics", is a professional skill and should be performed by suitably qualified personnel (*refer Paragraph 5*);
- detailed analysis of transactions, documents and files - "forensic accounting";
- analysis of calls made from office telephone and fax lines of suspect to identify non business related calls (i.e. calls to offshore banks, real estate agents and so on); and
- document forensics.

Leads obtained from the above actions will then be further investigated to develop all available evidence. At the conclusion of Stage 2, all statements and exhibits should be appended to a comprehensive report for consideration by senior management and (if appropriate) litigation lawyers, as a brief for further action.

In most cases, until the above actions are completed, YOU SHOULD NOT:

- suspend or dismiss any suspect
- question any suspect or witness
- make any unsubstantiated accusations

or take any other action which is likely to compromise the covert investigation.

Stage 3

Armed with the intelligence derived from Stage 2, you will be in a position to instruct lawyers to make ex-parte application to the Courts for:

- Mareva injunctions against the suspect (this has the effect of freezing assets and causing the suspect to disclose to the Court all assets wherever they may be).
- Anton Piller relief (this is a Court Order which permits lawyers for the aggrieved party to search the premises of the other side for specified documents) as well as other Court Orders which lawyers can rely upon in civil actions against the corporate fraudster.

Alternatively, you may prefer (and you may be required) to alert law enforcement authorities who will consider your claims and evidence before deciding whether to pursue the matter in the criminal arena.

Only when Stage 2 has been completed, and (if appropriate) Stage 3 is at the point of execution, should interviews with suspects be conducted. In all cases, it is imperative that suspects (both internal and external) are interviewed simultaneously to preclude the possibility of collusion. Interviews of suspects should *only* be undertaken by experienced interviewers.

Other Points to Remember:

Investigation management is vitally important. The person leading the investigation team should ensure that:

- a full record is made of the source of all documentary and other exhibits;
- a full note is made of all interviews including the time, place, persons present, etc.;
- interviews are legally tape recorded, where possible, to provide a true and complete record;
- the investigation is conducted fairly and confidentially;

and that all investigative techniques are absolutely legal in the various jurisdictions in which the investigation takes place.

Before an investigation is initiated, it is vital that serious consideration is given as to the choice of investigator. Fraud investigation is a specialist skill and is fraught with peril if performed in an unprofessional or haphazard fashion. Fraud investigations should not be conducted by management or others within your organisation unless they are sufficiently skilled and trained for the task.

6 COMPUTER BASED EVIDENCE RECOVERY

Traditionally the collection of evidence in a fraud investigation has relied upon the presence of a physical paper trail. In today's corporate environment, the paper trail largely originates from, and in many cases has been replaced by, personal computer records. In response to this trend, a field known as Computer Forensics has developed. Put simply, Computer Forensics is the seizure and analysis of electronic data using a methodology which ensures its future admissibility as evidence in a court of law. Computer Forensics is an integral part of modern fraud investigation.

The Forensic Image Process

The fundamental principle of Computer Forensics is that original data is NEVER altered. For this reason, purpose written 'forensic image' software is used to take an exact copy of a 'target' computer system. From this image the original system can be recreated at any time. It is essential that trained and experienced specialists are assigned to this task. This ensures both the integrity of the target system (it is difficult to put a monetary value on the accidental loss of commercial information), and the integrity of seized evidence. A Computer Forensic technician must be able to justify their actions in future court proceedings.

Forensic computer images have been accepted by Australian Courts to be 'original' evidence. It is no longer necessary (in most cases) to seize physical computer hardware. Indeed, in situations where target computer systems contain critical data, such as in a doctor's surgery, physical seizure is never a viable option. Once an image has been taken, hardware that may otherwise have been required to be secured for evidence continuity may be put back into use.

Forensic imaging is also well suited to covert investigations. Much information can be drawn from a suspect's personal computer without alerting him/her to an investigation.

Data Analysis

In the analysis phase, Computer Forensics is concerned with more than existing files. A Computer Forensic technician will examine the entire structure of a hard disk, looking to collect all possible evidence. During normal PC operation, data additional to that which the user intends to save is 'written' to the surface of the hard disk. On examination such information can be located as:

- ***File Slack:*** Part of a space reserved for use by a file that has not been completely filled by that file. This information consists of data pulled from the computer's memory, and used to 'pad' the file to the required length. Slack often consists of garbage text, but on many occasions has been found to contain text relevant to the investigation.

- ***Data Fragments:*** Units of disk space that are in use, yet are not accounted for by files on the disk. These fragments usually represent material left on the surface of the disk by old files or applications.
- ***System Slack:*** Data written to areas of the hard drive reserved for use by the computer's operating system. Some programs use this area as temporary storage.

  On many occasions valuable evidence from these areas has been collected from computer systems which were previously believed to be 'clean'.

In investigations where the suspect is computer literate, these areas are sometimes used to hide information. It is common that the actions of a suspect in removing or hiding evidence from a computer system can have the opposite effect, and strengthen the evidence. This is often the case with deleted files, or the non destructive 'format' of the computer hard drive.

In more recent PC-based operating systems, such as Windows 95 and Windows NT, there are a variety of 'cache files', 'swap space', 'audit logs', and 'registry entries' which all contain information about the actions of the user. An experienced computer forensic technician can quickly put together a profile of computer use, and identify potential evidence.

7 CONCLUSION

This paper is designed to give readers a broad overview of fraud prevention, detection and investigation techniques which have proved effective in the past. Naturally, some techniques will be more relevant than others dependent upon the industry and company involved. Organisations encountering fraud should take legal advice at a very early stage.

Taken together, these techniques should provide any organisation with an effective means of dealing with fraud risk.

ABOUT THE AUTHOR:

Malcolm Shackell is a director in the Fraud and Investigations practice of PricewaterhouseCoopers, Sydney. He is a CPA and is Vice president of the NSW Chapter of the Association of Certified Fraud Examiners.

PricewaterhouseCoopers Fraud and Investigations Practice consists of approximately twenty staff across Australia, with backgrounds in law enforcement, civil investigation, computer crime and accounting.

For more information concerning the issues discussed in this article, please contact Malcolm on (02) 8266 2993.

