Employee fraud

A guide to reducing the risk of employee fraud and what to do after a fraud is detected

CPA AUSTRALIA

CPA Australia Ltd ('CPA Australia') is one of the world's largest accounting bodies representing more than 132,000 members of the financial, accounting and business profession in 111 countries.

For information about CPA Australia, visit our website **cpaaustralia.com.au**

First published
CPA Australia Ltd
ACN 008 392 452
Level 20, 28 Freshwater Place
Southbank Vic 3006
Australia

ISBN: 978-1-921742-10-1

Legal notice

Contents

Introduction

Employee fraud is more common than most businesses think. It can have differing impacts on the success of a business. In the most serious of cases, employee fraud can lead to business failure and destroyed careers.

Misplaced trust, inadequate hiring and supervision policies, and a failure to implement strong internal controls create an environment that is ripe for an employee to commit fraud. Employee fraud is therefore about opportunity. Subsequently, businesses should take steps to reduce this opportunity.

The following guide includes:

- an overview of fraud, including common examples of fraud
- examples of strategies to reduce the risk of fraud
- information on what to do when a fraud is detected.

Businesses designing strategies to reduce the risk of fraud will have to balance their desire to minimise such risks with the business needs. In other words, a business must avoid becoming so focused on reducing the risk of fraud that it impairs the ability of the business to meet its commercial objectives.

What is fraud?

"Fraud is behaviour that is deceptive, dishonest, corrupt or unethical. For fraud to exist there needs to be an offender, a victim and an absence of control or safeguards."[1]

Fraud is generally described in three categories:

1. asset misappropriation
2. fraudulent accounting and financial reporting
3. corruption.

Conversely, fraudulent activity is usually motivated by one or more of three main factors:

1. pressures
2. opportunity
3. rationalisation.

Opportunity is the element that every business should be seeking to reduce.

1. *Your guide to stopping Employee fraud*, Queensland Police (www.police.qld.gov.au/Resources/Internet/programs/crimePrevention/documents/EmployeefraudBrochure.pdf).

The impact of fraudulent activities

Where a business is a victim of a fraud, there is more at stake than just the direct cost of the fraud. Other impacts to consider are:

- Staff morale can be affected as they feel a sense of betrayal that a colleague could do such a thing and/or management allowed the fraud to occur.
- Good employees do not want to work for a business where fraud is widespread, not investigated or not acted upon.
- The reputation of the business in the eyes of suppliers, customers, competitors, possible employees and other business partners (for example banks) can be damaged.
- Businesses may become overly internally focused in response to a fraud.
- For individuals that supervised the fraudster, the fraud can impact their reputation and therefore their career, particularly if the manager is in a financial role, as others will expect that given their expertise, they should have prevented the fraud.

Examples of fraud

Examples of employee fraud include:

- creating “ghost” employees or not deleting ex-employee records and having the salary of these “ghost” employees paid into the fraudster’s bank account
- creating bogus suppliers, with payment being made to the fraudster’s bank account
- creating bogus purchase orders of a bona fide supplier and substituting the supplier’s bank account details with fraudster’s bank account details
- obtaining kickbacks or bribes from suppliers or contractors
- associates of the staff providing services to the business at inflated prices
- personal use of business resources
- inflated/bogus reimbursement claims
- manipulation of financial data to receive performance based bonuses
- faking time sheets
- private purchases through business accounts/business credit cards
- providing discounted (or free) goods or services to friends and associates.

Strategies to minimise the risk of fraud

As the old saying goes “prevention is better than a cure” and this is certainly true when considering how to manage the risk of employee fraud. The most important aspect to managing this risk is ensuring that the business has solid internal controls in place as, for every fraudulent activity, there is always a breakdown of internal controls.

Minimising the potential for fraud will require designing and implementing internal controls that prevent, detect and deter most fraudulent behaviour. The successful implementation of such internal controls begins with the “tone at the top”. Managing the risk of fraud requires the business owners and senior managers to support and adhere to all policies and procedures implemented to manage this risk. The success of internal controls also requires that they be visible, built into the day-to-day work of the business and that employees are held accountable for their actions. In addition, internal controls should be continually reviewed and, where appropriate, amended.

It is important to realise that employee fraud cannot be eliminated but the risks of it occurring can be substantially reduced. The strategies to reduce the risk of employee fraud must strike a balance between the need for such controls and not “micro-managing” employees, therefore businesses will have to accept some degree of risk of employee fraud.

Through the implementation of some or all of the following strategies, your business can minimise the risk of becoming a victim of employee fraud.

Strategy	Description
Lead by example	Every person within the business, regardless of seniority, should adhere to the policies and procedures and be held accountable for their actions.
Create a positive working environment	A positive work environment encourages employees to follow policies and procedures, and act in the best interests of the business. Most employees will respond positively to clear organisational structure, clarity of job responsibilities, fair employment practices, open lines of communication between management and employees and positive employee recognition, hence reducing the likelihood employee fraud.
Have a policy manual	Ensure that your control procedures are documented and that every employee has access to the procedures and is trained in them. Reports on the implementation of the procedures should be made to senior management regularly. There should be a “zero tolerance” of breaches and adherence to the procedures should form part of the conditions of employment.
Create a code of conduct	The code of conduct should make it clear that there will be zero tolerance of any fraudulent activity on any level of the business and that any such fraud will be reported to the police. This code should also clarify what constitutes employee fraud, as this is often an area of confusion for employees.
Separation of duties	No one person should be responsible for a complete transaction from start to finish. For small businesses, where this is not practical, employees handling finance should be subject to close supervision.
Authorisation controls	Implement policies that clearly articulate who is authorised to conduct transactions on behalf of the business and who is responsible for each step of a transaction (including who has authority to authorise a payment over a certain amount or entering into a contract).
Implement a whistleblowing policy	Have a whistleblowing policy in place that outlines the steps to be taken if an employee suspects another individual of fraud. To supplement such a policy, a mechanism that allows employees to anonymously communicate their concerns about potential fraud is recommended. It is important that employees are aware that there will be no negative consequences when “blowing the whistle”. Management must also demonstrate that they actively follow up on all issues raised via the whistleblowing mechanism.
Create an organisational chart	Define the roles and responsibilities of all employees. This could include: job descriptions, reporting lines/segregation of duties, mandatory job rotations, authorisation policy and leave.

Strategy	Description
Implement a comprehensive recruitment policy	Make sure your recruitment policy involves: • past employment verification and seeking explanations of any employment gaps • police checks – there are specialist businesses that can provide this information within 48 hours • verification of qualifications – sight original documents or contact institutions that issued the qualifications • reference checks • credit checks, particularly for employees in finance roles and those handling cash • using technology to research potential employees, including viewing social networking sites.
Monitor employee behaviour	There are a number of employee behaviours that may indicate a heightened probability that an employee is committing fraud, including: • the employee regularly works outside of business hours or rarely takes leave. Although they may appear diligent, they may have other motives for being in the workplace unsupervised • the employee appears to be spending or living beyond their means • reports and reconciliations are not done (for whatever reason) • tax returns and other compliance forms are lodged late.
Implement supervisory processes	Strong supervision is vital, especially in smaller businesses that may have difficulty segregating duties. This can include approval, review, authorisations and occasional spot checks which might involve re-doing work.
Perform regular accounting reconciliations	Regular accounting reconciliations (such as bank reconciliations, payroll reconciliations and analysis between budget and actual figures) often make fraud concealment very difficult. The person doing a bank reconciliation should be different from the person doing the banking.
Implement physical access controls	Control physical access to premises, cash registers, computer systems, safes and other secure systems. For example: • ensure doors, desks and filing cabinets are locked • implement systems that report on employee activity, such as who has viewed and altered data in your database • consider installing electronic surveillance systems.
Investigate every incident	Gain the facts you need to make informed decisions and reduce losses through a thorough and prompt investigation of policy and procedure violations, allegations of fraud or warning signs of fraud.
Others	In addition to the aforementioned, employers should: • regularly review financial statements • deposit cash and cheques daily and make sure the person doing the banking is not the person collecting the money • secure blank cheques, signature stamps and access to EFT payments • never sign or authorise payments that are not fully completed • periodically check suppliers' details, including bank account details, with the actual supplier • only pay on original invoices • review billing error complaints from customers • engage an external accountant to audit their books • periodically compare payroll payees with employee records • ensure that all employees take annual leave during the year • have a cross training program in place to ensure that one employee is never the only person capable of a particular role • in instances where they use a personnel agency, check their contract with the agency to see whether the staff hired through the agency have been subject to a police check • question unusual accounting methods or unnecessary complexity in an accounting transaction or excessively long charts of accounts • bring in a contract accountant to fill in when their accountant is on leave.

What to do once fraud is detected?

Even with these checks in place, employee fraud can still occur (however the risk of it occurring is reduced).

If a fraud is detected, the immediate reaction from the business owner/management can often be emotional. An emotive response can compound your problems and give the fraudster the opportunity to take action against the employer in other ways (such as unfair dismissal). Taking a measured approach is the best way to deal with such a situation.

Step one: Stop the fraud continuing

The first thing to do when a fraud it committed is to stop it continuing. This involves:

- blocking or reducing access to electronic and other information or resources being used to commit the fraud, including blocking remote access
- if the employee has been using a computer, ensuring that the computer is isolated and no one else touches it. Forensic IT should be brought in to recover anything that has been deleted from the hard disk. In addition, email lists are often helpful in preparing evidence. The courts may not accept this evidence if there have been other users of the equipment. Backups can be useful during this process
- identifying other computers/equipment the employee may have used, and isolate these computers as well (even if it is another employee's computer).

Step two: Collect the facts

The second step to take after a fraud is detected is to make sure you collect as many facts as possible before you approach the employee. The employee may actually admit to committing the fraud once they learn you know what has been going on. Ensure that you speak to the fraudster's work colleagues. Often where a senior executive is involved in a fraud, their personal assistant has known about it but was unwilling to get involved. Employees need to know that they can safely discuss what they know.

Step three: Discuss the issue with the employee

The third step to take after a fraud is detected is to discuss the issue with the employee. However, you should be very careful and approach such conversations with a clear head. You may wish to seek legal advice before having the conversation or have your lawyer present to make sure it is done the right way. If you are in Australia, please read "Terminating an employee suspected of fraud in Australia" below.

The business may choose to let the employee resign rather than be terminated. However, it should be made clear to the employee that, whether the employee resigns or is terminated, the business will still report the fraud to the police and the business may still seek to recover the business's property from the employee through civil action.

Terminating an employee suspected of fraud in Australia

The following is provided by Katie Sweatman of the law firm Mason Sier Turnbull – www.mst.com.au. This information is correct as at February 2011.

Once a fraud is detected, care must be taken to ensure that no termination of employment of the suspected fraudster takes place unless there is reasonable evidence supporting the allegations of fraud. Therefore, take a deep breath before approaching an employee you suspect of committing a fraud.

If you intend to terminate the employee's employment with you, it is important that you take a measured approach to dismissing such an employee and that the dismissal is in accordance with the law. A surprise interview of the employee where dismissal may be discussed may lead to problems with unfair dismissal if procedural fairness is not followed.

Australia's unfair dismissal laws require that at any meeting where termination of employment may be discussed, the employee:

- know the reason for the dismissal and that they have an opportunity to respond to the allegations
- not be refused the opportunity to have a support person in the meeting where dismissal may be discussed.

If you do hold a surprise meeting with the employee where accusations of fraud are levelled at the employee (but where dismissal is not discussed), the business should give the employee the opportunity to:

- consider the information presented before them
- seek advice
- bring in a support person to the next meeting.

You should also let the employee know that, at a subsequent meeting, you will discuss with them how you are going to handle the allegations.

If the employee admits to committing the fraud at the initial meeting and accepts the consequences without the need for a subsequent meeting or a support person then you, as the employer, can act on the dismissal. However, you must inform the employee of their rights to seek advice and have a support person present. If the employee chooses to waive such rights, you should keep a detailed diary note of that.

An alternative to dismissal is to suspend the employee with pay at any time while the fraud is being investigated.

Fraudulent or illegal conduct may override employment contract provisions, including notice of termination requirements. However, the employee's superannuation, leave and long service entitlements, subject to the state where the employment takes place, may not be withheld as compensation, as those entitlements have a statutory basis.

If the termination is done effectively and fairly, it may also increase the chances of you getting information from the employee that will help your investigation, which, in turn, can assist police.

If you have any concerns with terminating or suspending an employee please contact Mason Sier Turnbull www.mst.com.au or your lawyer.

Step four: Report the fraud to the police

The fourth step to take after a fraud is detected is for the business to report the fraud to their local police station. If the matter is left unreported, the fraudster may commit a fraud on another business and your inaction may further damage your reputation with employees, potential employees, suppliers, customers and your bank.

To assist police with the investigation, it is advisable that the business spend some time collating evidence into a brief for the police.

The following is a guide to what information to give to police when reporting the fraud:

Details of employee who has committed the fraud	Supply name, address, date of birth, contact phone numbers, email and employment details, including start date, leave dates, vehicle registration, passport details, licence details.
Summary of allegations	Prepare a summary of events in chronological order that forms the basis of your allegation. Include times, dates, places and any conversations or interaction with suspect regarding the allegation.
Evidence	Include a brief description of the evidence that supports the events described.
Witnesses	Provide details of any witnesses, including their name, address, phone number and a brief summary of why this person is a witness.
Document/exhibits	Provide copies of documents or exhibits which support the complaint. This may include, but is not limited to, banking records, business records, receipts, contracts, invoices, internet content, phone records and audit reports. Treat original document with care as this may be used as evidence.
Action taken against suspect	Provide information of any discipline or civil action taken against the suspect/s.

Case studies

Case study one: Wholesale distributor with national network

Within one month of beginning employment, the employee began creating fictitious invoices randomly from three large suppliers, and paid them within the month the invoice was raised. Thus, the invoices did not show up as creditors on potential audit reconciliations. The electronic payments on these fictitious invoices were made direct to the employee's own bank account. The employee that committed the fraud was selected through a personnel agency from a short-list of candidates, with no police check.

The finances of the business were managed by one person. Management personnel were focused on statistical sales reports and inventory control and therefore the employee that committed the fraud focused on providing such reports. This satisfied the information needs of management. Financial reports against budget were required but not produced regularly by the employee. In essence, the employee was not supervised in regard to general office administration.

The fraud was detected within 12 months of employment commencing.

The internal checks that discovered the fraud were instigated by the directors/owners because:

- there was a significant over-run in the cost of goods sold (actual versus budget)
- the monthly profit performance reports were not being produced as requested by the directors/owners.

When confronted with a preliminary reconciliation of the "missing funds", the employee confessed and pleaded for the employer not to report them to the police. However, the person was immediately dismissed and a report was lodged with the police. There was frustration from the employer because of the perceived lack of speed by the police in dealing with the matter. This was compounded by the lack of response from the employer's bank in identifying transactions beyond the last three months.

Case study two: Telecommunications business

The business recruited a sales manager to reorganise and expand their business into new geographic areas. The successful applicant had two degrees and a masters (MBA). The employer was very impressed that they could recruit such a well qualified applicant at a relatively low salary.

The employee:

- set up a channel program to expand the business into a new geographic area
- expanded the range of products the business sold
- expanded the business into retail.

A number of alarms bells alerted the business that something was not right, including:

- The business had to send the employee on an Excel course as the employee's spreadsheet skills were very poor. This did not equate with someone who was so well qualified.
- The employee explained to management that to expand into retail in their particular industry required the business go through a particular distributor and to secure a relationship with that distributor, they had to give them $10,000 in cash.

Things started to not add up. The business started to do further background checks on the employee, including asking their lawyers to contact the education institutions the employee claimed to have graduated from. These checks uncovered that the employee did not have the qualifications they claimed to have. Upon discovering that the employee had falsified their qualifications, the business dismissed the employee immediately.

Further investigation by the business discovered the employee:

- had organised "kickbacks" with suppliers of the new of products
- was receiving payments from a channel partner that the partner thought was being made to the business
- was stealing partner incentive stock, including expensive electronic equipment
- did not have a prior criminal record.

Two days after the employee's dismissal, the employee had found new employment and was seeking to establish the same arrangement with one of the suppliers the employee had established for the business. The business knew the new employer and recommended that they check the veracity of the employee's qualifications.

The business pulled together all the facts and gave those facts together with an executive summary to the police. Once interviewed by the police, the employee admitted to the fraud. Even though the employee admitted to the fraud, it took almost a year to prosecute the employee.

The business now requires applicants to bring in original certificates of qualifications and the business also checks with prior employers as well as stated references, to confirm periods of employment and the applicant's title.

CPA187435 03/2011

cpaaustralia.com.au

CPA AUSTRALIA