

WORKPLACE FRAUD

- Electronic theft in the workplace
- Preventing fraud
- Investigation and detection
- Restraining fraud

1. Electronic theft in the workplace

The ease with which data can be downloaded conveniently and quickly onto portable, high capacity storage devices or emailed across the internet makes them a common culprit for data loss and an attractive means for data theft.

Mobile devices such as phones, USB sticks and even iPods have the capacity to store thousands of Word documents, emails and client contact details. Laptops, particularly where an employee has remote online access, give employees access to substantial confidential information belonging to their employer.

Most employers rely on very basic security measures, such as passwords, to prevent inadvertent loss of mobile data, while there is little and in many cases no protection against intentional data theft by an employee.

In *Luxottica Retail Australia v Grant* [2009] NSWSC 126, the New South Wales Supreme Court considered the claim of an employer for damages after it detected a departing employee had emailed documents to herself and to her husband, who worked for a competitor.

The employee was an optometrist employed by Luxottica, which operates the OPSM brand. She approached OPSM's competitor, Specsavers, in April 2008, to express interest in working for the company. It offered her a job on August 25, which she accepted the following day.

Before she informed her employer of her resignation, the employee forwarded 23 emails to her home email address and one to her husband who also worked for Specsavers. The emails included four documents which had substantial confidential and copyright material belonging to the employer. The employee also forwarded to herself the contact details for 12 OPSP employees.

The employer discovered the email trail and immediately removed the employee from the office. Early detection of the breach and expeditious action by the employer to prevent her from using the information restricted the damage to the employer.

The employer brought a claim alleging breach of the confidential information provision of the contract and breach of copyright.

The employer was able to rely on express provisions in the employee's contract preventing her from copying, using or disclosing confidential information both during and after employment, as well as its policies relating to employee's internet and email use.

The Court found that the employee breached her employment contract and that she infringed the company's copyright. The Court granted orders restraining the employee from altering, deleting or disposing of the computer files and awarded the employer nominal damages of \$10.

The case is a timely reminder of the need to take immediate and urgent steps to minimise damage as soon as an employer becomes aware of any breach of data security and the importance of appropriate clauses in contracts of employment, and internet and email policies, particularly in states where employers must comply with workplace surveillance legislation.

There are other forms of fraudulent methods that employees use to obtain payroll money from an employer on a fraudulent basis:

- **Swiping in absence:** The employee arrives at the job site at the beginning of the shift and swipes in to report to work. The employee promptly departs, and his or her absence goes unnoticed in a large workplace. At the end of the shift, the employee returns to swipe out.

- **False signature:** The employee who is supposed to obtain a supervisor's signature to verify having worked signs the form him or herself after not having reported to work. Such acts are usually possible with temp agencies, where contractors are sent to a variety of job sites, and are not known personally by those they would work with.

- Fraudulent medical certificates: The employee uses the same medical certificate on more than one occasion, by amending the date and providing the employer with a fax copy, rather than the original.

2. Preventing Fraud

There are actions which can be taken to manage an organisation's exposure to fraudulent activity in the workplace. Implementation of policies and procedures is the first fundamental step in prevention of fraud. Policies aimed at fraud prevention might include:

- Appointing an executive level member of management responsible for fraud risk management;
- Formalising roles and responsibilities of the board, management and staff;
- Involving personnel at all levels;
- Conducting risk management assessments;
- Independent reviews of contracts to monitor the performance of suppliers.

A workforce audit is one of the most effective ways for employers to identify and respond to risks in the workplace. Such an audit would involve a comprehensive review of all aspects of managing a workforce, including assessment of opportunities for fraud, as well as legal compliance of company policies.

2.1 Recruitment procedures

To earn a mark for best practice in hiring staff, you must have a clear job description for each position you are recruiting for, including key outcomes and/or performance indicators. It is essential that your employment contracts correctly reflect the nature of the job and address legal requirements such as probation and notice periods.

Fraud risks in recruitment include:

- Fake credentials: Some applicants provide false documents that are required or strongly recommended in order to obtain a job. These may include a degree, license, certificate, or other evidence of necessary training or experience that is expected of applicants.
- Fictitious former employer(s): The applicant provides a list of one or more previous employers that he or she never worked for, and that may have never existed. Included could be fake reference letters vouching for the applicant. Excuses for the absence of a way to contact them may seem plausible – no longer in business, living far away, or otherwise out of touch.

- Fake "live" employer(s): The applicant arranges with a relative or friend to pose as a former boss. The applicant provides a phone number or other contact information, and when the prospective employer contacts this person, he or she receives a glowing report about the applicant. Since the widespread use of email, this form of communication may also be used by the applicants themselves to pose as former employers.
- Exaggerated claims: The applicant lists a former employer he or she has actually worked for, but leaves out other information with the intent to mislead. Though the employer itself may have a prestigious reputation, the applicant's position may have been menial.

Employers must also take care to avoid employees giving references in relation to a co-worker on behalf of the employer, without proper authority. Permitting employees to give reference without proper authority gives rise to a risk to the employer of being held liable for a falsely positive reference, or in defamation if the reference is unfairly harsh.

In *Spring v Guardian Assurance* (1994) 3 All ER 129 the House of Lords found that a previous employer owed a duty of care to the plaintiff (a former employee) when preparing a reference and was liable for damages for any economic loss suffered by him because of its negligent preparation.

3. Detecting Fraud

It's important that investigations are carried out quickly and a conclusion reached as soon as possible.

3.1 Legally compliant workplace surveillance

Surveillance of employees in the workplace can involve video or audio surveillance, and monitoring use of email and internet, provided the employer does not cause trespass or nuisance. There is an ever-increasing range of laws designed to regulate the use of workplace surveillance. Each Australian state has different approaches and some states have even outlawed its use.

In Queensland, there is no particular restriction on the use of workplace video surveillance or computer monitoring. However, employers must take care to manage employee personal information in accordance with the *Privacy Act 1988* (Cth) and avoid breaching criminal laws prohibiting the recording of conversations under the Federal *Telecommunications Acts*.

3.2 Effective internal reporting and investigation process

Characteristics of good internal procedure include:

- Crucial that all employees made aware of complaints procedure - both when they commence work and on an ongoing basis.
- Procedure should be in writing and should be in plain English so people know where they stand – could be a stand alone document or be built into a general policy.
- Should state who will conduct the process.
- The complaints procedure should have alternative contact people for employees to approach with their complaint – it's important that an employee isn't rebuked for going over the head of their immediate superior.

If the employer does come to the conclusion that the employee is guilty of fraud then careful consideration has to be given to the appropriate form of punishment. This depends upon the degree of the misconduct, and it ranges from minor misconduct warranting a written warning on the employee's file up to possible termination of employment in many cases.

4. Restraining Fraud

4.1 Intellectual property

The law provides legislated and common law protection to prevent employee fraud in relation to some types of intellectual property. Protection of intellectual property takes several forms including –

- Trade marks
- Copyright
- Restraint of trade
- Confidential information

Conducting an audit of what intellectual property the business relies upon is a significant first step in ensuring it is protected. An IP audit is a systematic review of the IP created, owned, used or acquired by a company. When undertaking an audit a number of issues should be addressed including identifying IP and understanding the ownership and licensing arrangements in place.

An audit will provide an assessment of the type of IP education staff require and the type of information which may need additional protection through employment contracts.

Protection against trade mark fraud is available under the *Trade Marks Act 1995* (Cth). In addition, protective measures are also available under the *Copyright Act 1968* (Cth).

The *Copyright Act* protects original written works including webpage design, articles, even job advertisements in some circumstances. As soon as the 'work' is fixed in material form, i.e., written down, the right to enforce copyright arises automatically without the need for registration of any kind. A copyright notice is not required but is a useful attribution of copyright ownership and a warning to potential infringers.

4.2 Confidential information

Employees are entitled to use the skills and knowledge learned in their employment in their future work. They are entitled to take with them information about the markets in which a former employer operates and skills relating to management processes and outcomes learnt in the former employment.

However employees are not entitled to copy and remove, or memorise, information which is confidential to the business. Information that is obviously confidential includes trade secrets or client lists, but not necessarily marketing plans, pricing policies or costings.

In addition to statutory protection, a breach of confidence action may be available to protect trade secrets and confidential information from being exploited outside the business. However, it is limited to information that is genuinely "confidential" or "secret", such as client proposals, customer and price lists, and marketing strategies. It does not extend to know-how that an employee may develop in the course of employment. For that reason, it is useful to include express provisions in the contract of employment identifying and dealing with confidential information.

In the case of professional staff, it may be necessary to expand what is to remain confidential by a term of the employment contract. A client database is an example of information that may be confidential and capable of extra protection through an employment agreement.

4.3 Restraint of trade

Restrictions on employees working in competition with their employer during the period of their employment are almost always enforceable. However an employee is free to lawfully leave their present employment and accept work with a competitor or establish a business in competition.

The freedom to work in a competing business raises questions about the ability to protect confidential or sensitive business information, such as the identity of clients and database information.

In addition to restraints on the use of confidential information, a restraint of trade agreement entered into at the commencement of employment, can limit an employee's freedom to work for a competitor or prevent them from setting up a competing business within a specific time period.

The general rule in relation to restraints is that any restriction on an employee taking alternative employment or establishing a competing business after employment has ceased, is void and unenforceable. However, a former employer may enforce a restriction if it is able to prove that the restraint is reasonable, having regard to its legitimate business interests and what is reasonably necessary to protect those business interests.

The enforceability of such a restraint depends on whether it meets the test of "reasonableness" in protecting the employer's legitimate business interests. In assessing this, the court will consider:

- The geographical area of the restraint;
- The time period of the restraint;
- The scope of activities which are restrained.

From the perspective of an employer seeking to impose an enforceable restraint, it is sensible to seek only the minimum restriction which will protect the employer's interests. For example, it may be necessary to restrain a CEO from working in a competing business for several years, but it is unlikely the same term could be imposed on a sales person with no managerial responsibility.

Although it may seem an attractive option, a restraint that seeks to prevent an employee from working anywhere in the relevant industry for 12 months will be invalid. However a restraint that prevents an employee from soliciting work from clients of the former employer for 3 months is likely to be valid. While the first might seem ideal to prevent employee poaching clients, if it is unenforceable it is of no practical value.

Consider the business imperatives – in many cases a period as short as 3-6 months is a sufficient period of time to secure a client.

Rachel Drew

Partner, Macrossans Lawyers

T + 61 7 3292 9717 F + 61 7 3292 9799 E rdrew@macrossans.com.au

www.macrossans.com.au

GPO Box 2763, Brisbane Q 4001

Level 23, AMP Place, 10 Eagle Street, Brisbane Q 4000

A member of the Hunt & Hunt Legal Group

Court multiplies lost profits four-fold, in bid to remedy damage to employer's business

01 April 2009 1:44pm

A court has ordered two workers to pay more than \$200,000 in compensation to their former employer, after finding they caused him to lose earnings and to sell his business at a discount when they covertly went into competition with him and diverted custom while still in his employ.

The service manager and installer employed by telecommunications dealer SkyComm set up a partnership call DapComm in July 2004 while still employed by SkyComm. The service manager resigned 10 months later when SkyComm's proprietor became aware of DapComm's activities, while the installer worked under contract for various periods during 2004.

The Queensland Supreme Court heard that the principal of SkyComm had identified the service manager as his "heir apparent" and had given him full access to confidential files about its customer base since early 2004.

Justice Anthe Philippides said the employees had a duty of good faith and fidelity to Skycomm and that they were not entitled to "use knowledge or opportunities or other advantages arising out of their employment to make a personal gain without SkyComm's consent".

She found the service manager and installer had "acted secretly to set up a business in competition with [SkyComm], in circumstances where [the service manager] diverted custom to the partnership through opportunities which were made available to him by virtue of his employment with [SkyComm]".

The service manager also profited by using SkyComm's premier Motorola dealership, placing orders to benefit Dapcomm and compete with SkyComm, Justice Philippides held.

She also found the service manager canvassed SkyComm's customers, breaching his duty not to act to the detriment of Skycomm.

Justice Philippides also inferred that the service manager continued to pursue the secretly-obtained commercial contacts and canvass SkyComm customers after he left the company.

Damages formula based on sale price

The court awarded damages firstly for the losses to the business's earnings and secondly for the reduction in the price gained by Skycomm's proprietor when he sold the business in late 2005.

Justice Philippides said the business had been sold for \$650,000 in late 2005, with the price a multiple of 3.8 times earnings before interest and tax (EBIT).

EBIT in the year up to the sale had been \$170,000 - well below the average for the three previous years of about \$305,000.

The sale price had been lower than it otherwise would have been, because EBIT had been lower than in previous years, due partially to the activities of the two former employees.

The judge applied the same formula for damages as had been applied for the sale, taking the \$38,000 in profits that she had accepted had been lost, and multiplying them by 3.8, to provide compensation of \$145,000 for the reduced sale price.

Justice Philippides also ordered the former employees to pay \$67,500 in damages for the loss of profits due to their activities, making a total damages payout of \$212,000.

Sale price/formula provided vital evidence of losses

McDonald Balanda and Associates lawyer Warwick Chesters said the unique feature of the case was that the business had been sold soon after the problems caused by the employees had emerged.

"This enabled the judge to accept the business purchaser's evidence that the downturn in profit caused the purchase price to be dropped.

"She could therefore use the multiple of EBIT used in the sale to establish the sale price, in the assessment of damages.

"However, there was still imprecision in the assessment of the true damages as it is usually impossible to assess what the employees actually did after they set up the competing business.

The judge would only apply the multiple to the losses she felt comfortable apportioning to the employees' actions", he said.

[Dinte v. Hales & Anor \[2009\] QSC 63 \(25 March 2009\)](#)