



For Immediate Release  
29 May 2009

For More Information Contact:  
Ralph Lake  
0418 708 340

## **Businesses Especially Vulnerable to Fraud**

Fraud is a universal problem that threatens the very underpinnings of business and government across the globe.

Fraud doesn't involve just money. There are three main categories of fraud in the workplace: Asset Misappropriation; Fraudulent Statements; and Corruption. Each of these categories involve both cash and non-cash frauds.

The interesting thing about fraud in the private sector is that if fraud is uncovered, most companies do not prosecute. Moreover; individual restitution agreements are made with employees.

As the financial crisis continues to unfold, new suspicions of fraud have been emerging, and with them a need to find whether there is evidence of wrongdoing. It is perhaps not surprising to learn then that the demand for fraud investigators is rising.

Many frauds have remained hidden during the boom years but due to the economic down turn the tide is going out and exposing everything that it has left behind.

With all of the corporate scandals that have been going on in recent years, corporations have been developing compliance programs to keep them out of trouble when employees deviate from acceptable behaviour. So how does your corporation measure up? If it's not top in order, you may find yourself in hot water if corporate mischief occurs.

Most organisations can't do the job themselves because they don't have a specialised fraud detection and prevention unit. Many organisations have had fraud prevention programs that didn't work and didn't protect their firms, their employees, or their shareholders from the devastating charges and resultant publicity. Where were the fraud prevention basics that should have been in place?

Pay lip service to fraud prevention and it will bite you!

Unfortunately many high-profile corporations have learned the hard way about the devastating effects of fraud. Even though some may have had internal units to deal with this they couldn't do anything to protect employees and shareholders from executives determined to loot their own companies.

All entities, “including yours” need robust fraud prevention programs overseen by with savvy and cunning fraud examiners. For most firms, fraud examination is not a core business component. That's why, when fraud is suspected or discovered, it is imperative to enlist the anti-fraud expertise of a Certified Fraud Examiner (CFE). The CFE credential is recognized by businesses and governments worldwide as the standard for fraud prevention and detection. To locate a CFE in your area, visit [www.ACFE.com](http://www.ACFE.com).

The ideal fraud prevention program will protect a company from itself by:

- instituting a whistle blowing program;
- setting the principled tone at the top;
- developing a code of conduct;
- creating a positive environment;
- hiring and promoting appropriate employees;
- instituting continuous training;
- having fair and balanced discipline;
- identifying and measuring fraud risks;
- implementing and monitoring internal controls;
- having a strong and independent audit committee;
- hiring effective internal auditors and Certified Fraud Examiners;
- contracting independent external auditors;
- constructing a Fraud Investigation/Financial Integrity Unit;
- using case management and technology tools; and
- emphasizing cross-group collaboration.

An ounce of prevention is worth a pound of cure!

While internal audits, external audits and background checks also significantly reduced losses, the greatest reduction in loss was associated with anonymous reporting or whistle blowing mechanisms.

Beyond the obvious financial benefit of stopping fraud in its early stages, a whistle blowing mechanism, such as [www.disclose.com.au](http://www.disclose.com.au) or a hotline, can give a company the opportunity to limit liability of offences by uncovering and dealing with issues long before they are exposed in the media and can protect a company from the destruction of goodwill in the eyes of investors, customers, and other stakeholders.

If you're considering implementing a whistle blowing mechanism you will need to communicate to employees about behaviours that aren't acceptable, and how to report them. A comprehensive program includes periodic communication to employees and others about the behaviours that are acceptable and unacceptable. This communication should include everything from articles on the company intranet site to posters in lunch rooms to discussions at company meetings. This type of communication reinforces everyone's perception that the company wants to uncover illegal and unethical activities and address them.

Encourage employees to use internal channels, but let them know they can remain anonymous by using the hotline. Analysis of more than 47,000 incidents reported via hotline calls in 2002 showed that 48 percent of callers chose to remain anonymous. (Source: The

Network Inc. internal data) This number may seem high, but it may be explained by another statistic: 33 percent of hotline callers previously had reported the incident to management.

The implication is that although the employee reported an incident, his or her manager either failed to follow up, or the employee wasn't happy with the results. Take the case in which the caller's own manager is involved in the cover-up of serious misconduct. The anonymous report gives the company a chance to intervene in a potentially volatile situation, possibly preventing a costly legal action. An entity that's serious about preventing fraud will make every effort to give people an option for reporting that makes them comfortable. Many companies are adding a third-party provider of these services in addition to an internal hotline to make sure they have given employees every avenue for reporting malfeasance to the company rather than contacting an outside party like a lawyer or the media.

Make the whistle blowing mechanism available to all of those involved with your business, not just employees. To be most effective, a whistle blowing mechanism must be comprehensive, involve employees, suppliers, investors, and customers. Different groups of people, like vendors, may be aware of different types of fraud. For example, employees of vendors might report fraud in the form of over-billing, while others may report other types of fraud. One way to reach the accounting employees of your suppliers is by printing the whistle blowing mechanism details on purchase orders and invoices you print.

Create a plan that ensures that reports are sent to the right people. A report dissemination routine should be set up with the whistle blowing administrator so that issues like harassment are sent to human resources and/or legal departments, while issues like fraud or breaches of the Corporations Law are sent an appropriate representative.