



Business Security

The safety of your business, employees and customers should be of paramount importance. The information provided in this leaflet is designed to assist you to reduce the prospect of crime and the chances of your business becoming a target.

Assets, inventory and staff belongings can be at risk of theft or vandalism, if measures are not taken to minimise the risk.

Fraud

All businesses can be susceptible to fraud, but the nature of the fraud will vary according to the type and location of the business.

A common source of fraud is new and unknown suppliers or customers. Another widespread issue is internal theft, particularly for retail businesses.

Small businesses do not need to develop a sophisticated fraud prevention strategy, but a simple survey of security risks and practical, cost effective strategies could prevent considerable loss. Your fraud prevention survey and strategy could cover the following areas:

1. New Suppliers and Customers

Check out new suppliers and customers that have requested credit.

A useful first step is to find out who owns the business you are dealing with. You can do a search on current and former companies, business names, schemes, trusts and non-registered entities on the National Name Index through the Australian Securities and Investments Commission (ASIC) databases available on their website (www.asic.gov.au).

You may also search for disqualified persons or do personal names search on company directors/officers of registered companies in Australia on the ASIC website. ASIC also provides guidance and services to assist you. For more information contact ASIC on 1300 300 630 or visit their website at www.asic.gov.au.

2. Cheques

To ensure that your cheques are not stolen or misused, make sure that:

- ✓ cheque books and credit cards are kept in a secure place in different locations

- ✓ your address and phone number are not written on the back of cheques
- ✓ blank spaces are not left on cheques

To ensure that you do not accept fraudulent cheques it is best that you enforce a policy for acceptance of cheques and cheque limits, such as:

- ✓ witness your client re-signed cheques and that signatures match when receiving pre-endorsed cheques
- ✓ always verify cheques for the correct signature and date, any changes made, and inconsistent handwriting
- ✓ contact the bank for clearance of large cheques, particularly for new customers.

3. Credit Cards

To guard against credit card fraud, you should routinely check:

- ✓ the quality of the hologram, that there is a clean and even printing and embossing, the consistency of commencement and expiry dates and that the signature has not been altered or smudged; and
- ✓ the signature on the sales strip matches the signature on the card

The card should not be returned to the purchaser before the sale is processed and signature confirmed.

4. Scams

A scam is a fraudulent trick. To play it safe, it is best to deal with people who you know or companies that are known or trusted. Otherwise take the time to investigate new customers and verify their identity.

When doing business, provide written information for quotes made. Also take the time to carefully read and discuss all contracts with your solicitor and/or accountant, particularly if significant money, time or responsibility is involved.

To protect yourself from scams:

- Obtain a copy of *The Little Black Book of Scams* Contact the NSW Office of Fair Trading on 13 32 20 or email publications@fairtrading.nsw.gov.au. Also visit their website at
- www.fairtrading.nsw.gov.au.
- Contact the Australian Competition and Consumer Commission on 9230 9133 for advice or to report a scam.

5. Internal Theft

All businesses face varying degrees of internal theft. It is advisable that you have clear and well-communicated procedures for:

- ✓ Staff selection, including checking references and criminal records
- ✓ Disclosure of keys, access codes to alarms, safes and computer systems
- ✓ Handling, storing and accounting for cash in the cash register, safe and bank
- ✓ Staff purchases and discounts
- ✓ Employee responsibilities, expected behaviours and actions

6. Data Security and Computer Hack Attack

To guard against computer damage and electronic fraud, make sure you:

- ✓ Install and regularly update firewalls and virus protection software in the computer network
- ✓ Regularly change your passwords
- ✓ Have your computer system independently reviewed, addressing any security risks
- ✓ Ensure that you only conduct internet transactions that have secured processing

7. Counterfeit Notes

Counterfeit notes are an irregular but real risk for small business. Staff should be trained to check and recognise fake notes. Refer to the Reserve Bank of Australia website (www.rba.gov.au/CurrencyNotes/) for tips on detecting counterfeit notes and identifying security features in genuine currency. Incidents involving counterfeit currency should be immediately reported to the Police or to the Reserve Bank.

Burglary

Burglaries are generally the result of people taking advantage of opportunities. It is therefore important to ensure that your premises are as secure as possible.

- ✓ Fit security devices such as deadlocks and alarms on windows and doors.

- ✓ Keep keys in secure places and replace locks if keys go missing.
- ✓ Store valuables in a locked safe or secure room.
- ✓ Keep minimal cash on the premises and bank regularly. If possible, use a professional cash service.
- ✓ Engrave, mark or photograph rare and expensive items and keep record of equipment make, model, description serial number and value in a register.
- ✓ Lock your mailbox or if possible, rent a mailbox at the local post office.

Other Security Issues:

1. Fire

Fire is a common risk and when it occurs, the disruption to a business can be crippling from loss of income, loss of important documents, information and data.

To minimise this risk, undertake a survey to identify the most likely causes of fire in your business and develop a plan for addressing any issues. The survey should cover all locations and the following items:

- evacuation routes and procedures, fire extinguishers/detectors/sprinklers and fire doors;
- electrical outlets; rubbish management; and flammable liquids storage.

For more information and advice, contact the NSW Fire Brigades on 9265 2999 or visit www.nswfb.nsw.gov.au.

2. Staff and Customer Injury

At least one person on duty needs to have a current First Aid qualification. You should also regularly check first aid supplies to ensure that there is an adequate quantity and that they are up to date. Contact St John Ambulance Australia on (02) 9212 1088 for advice.

3. Bomb Threats

Contact the NSW Police Service on 1800 622 571 for appropriate guidelines and procedures.

4. Terrorist Threats

If you have concerns over any activities that may be relevant to Australia's security, call the National Security Hotline on 1800 123 400. The National Security Hotline also provides information on a wide range of national security matters.

For more information about Australia's National Security measures, visit www.nationalsecurity.gov.au.