



AUSTRALIAN BANKERS' ASSOCIATION INC.



ASIC

Australian Securities & Investments Commission

Protecting Your Customers

Businesses have a vital role to play in managing personal and sensitive information that they have access to; they are the key to controlling the invasive crime of identity theft.

The following areas should be considered with regards your business' information handling security:

- **Information acquisition** – Do you need the information that you gather? Are you acquiring it in a safe manner?
- **Storage** – What computer security measures have you placed around the systems storing personal data? Is the data considered highly classified with limited access? Do you keep all personal data (paper files) about employees and customers in locked cabinets?
- **Access** – Who has access? Is personal identifying information available only to limited staff? Is your database access audited or password controlled?
- **Disposal** – What is in your garbage bin? Is it a treasure chest for thieves? Are electronic/paper documents and databases containing personal information rendered unreadable prior to disposal?
- **Distribution** – Are staff trained in the proper procedures regarding information disclosure? Do you publicly display, use or exchange personal information in your workplace? This includes employee or membership cards, timecards, work schedules, licenses or permits and computer access codes.
- **Staff** – Do you conduct regular background checks on ALL employees with access to personal identifying information? Such as cleaners, temp workers and computer or hotline service technicians. Are staff trained in your security procedures, do they know how to securely gather and store personal information. Do they know what information can be sent by fax, e-mail or released over the phone?
- **Environment** – Do you provide a secure environment for your employees? Are their personal belongings hidden from public view and in a safe place?

Important Note: This fact sheet gives information of a general nature and is not intended to be relied on by readers as advice in any particular matter. We suggest that you consult your financial planner on how this information may apply to your own circumstances.

Your privacy obligations

Businesses have significant obligations to protect the personal and business information and records at its disposal. It is not an acceptable excuse to claim that these records only came into risk through the actions of a hacker.

Small business owners are obligated to protect the information in their custody. This includes adhering to the following laws:

The Privacy Act: Your business may be required to protect the personal information it holds from misuse and loss, unauthorised access, modification or disclosure. Serious fines apply for non-compliance or a careless attitude.

Corporations Act: Under the Corporations Act 2001, you must have 'adequate protection' over information at your disposal. Also, the Corporations Act imposes obligations to keep copies of business records for a number of years.

Trade Practices Act: Another party may sue the business operator if they incur loss or damage through a security breach at your business.

Directors' Liability: A director is obliged to protect the corporate assets at their disposal, otherwise civil, Australian Securities and Investments Commission (ASIC) and criminal proceedings may result. As most small businesses now have some form of corporate entity structure or protection, this is now more relevant.

Criminal Liability: If delegated employees act in a criminal manner, the business operator may be held responsible for their activities.

Card Schemes: Under card schemes such as MasterCard and Visa, merchants are responsible for keeping all customer information safe and secure. If a merchant site is identified as a point of compromise this may result in heavy penalties and/or termination of merchant facilities.

December 2006

Web: www.protectfinancialid.org.au Phone: 02 8298 0417 Fax: 02 8298 0402