AUSTRALIAN BANKERS' ASSOCIATION INC.

<AHTCC>

ASIC
Australian Securities & Investments Commission

Practical Prevention Tips

- **Provide only necessary information** about yourself. Sometimes businesses request large amounts of information they don't need.
- **Destroy personal information** such as bills and account statements by tearing, cutting up or shredding before throwing them away.
- **Lock your letterbox**. If you are away from home for an extended time, have your mail held at the Post Office.
- **Check you've received all expected bills and statements.** A missing letter could indicate a thief took it from your letterbox or changed your billing address.
- **Sign all credit and debit cards** as soon as you receive them.
- **If you move house** tell your bank, card issuer and other organisations that you deal with immediately. It is also a good idea to tell them if you have changed telephone numbers, so they can contact you if they notice suspicious activity on your account.
- **Securely store personal information** at home. This could include a list or photocopy of all your credit cards, debit cards, bank accounts and investments – the account numbers, expiration dates and emergency contact details. It is important to act quickly if personal information is compromised. Do not store this information in your wallet or purse.
- **Use your common sense**. If it looks to good to be true, then it most likely is.
- **Try to keep your receipts and thoroughly check your account statements as soon as they arrive**. Follow-up any unfamiliar transactions. When shopping put your receipts in your wallet rather than in the shopping bag.
- **Don't leave personal documents that contain your address in your car glove box**.
- **Consider limiting the amount of credit you have in your account.** Also consider whether it may be safer to use a separate credit card account for online transactions and when you are overseas.
- **Have passwords for your** handheld electronic devices, such as mobile phones and PDAs.
- **Read the privacy policy** before providing information to any business to ensure you understand how protected your data will be.
- **Collect your new credit card and cheque books in person** rather than by mail. If that is not possible, watch out for them and phone your bank if they haven't arrived when expected.

For more information on protecting yourself refer to the fact sheets *Protecting Yourself Online* and *Purchasing a credit file – is it worth it?*

How do banks protect my personal information?

Banks use a combination of safeguards to protect your information such as employee training, privacy policies, security and encryption systems. They have systems in place to constantly monitor transactions and if a transaction is identified as suspicious, it will be investigated to ensure there is no breach of security. Occasionally, this may involve a bank staff member contacting you to verify a transaction.

Bank customers are protected from loss in genuine fraud cases. Account holders are not liable for losses resulting from unauthorised transactions where it is clear that user has not contributed to the loss. There is usually an investigation by the bank to determine how the fraud has occurred.

Banks are continuing to seek out security enhancements especially for online banking, such as an on-screen keypad which is designed to prevent the incidence of keystroke logging fraud by removing the need for a keyboard to enter in passwords. Other banks are offering what's called two-factor authentication. An example of one factor authentication is the use of a password to enable access to Internet banking.

Two-factor authentication requires two independent authentication steps for a customer to access Internet banking. Customers will authenticate their identity and access to the system twice, first with something they know and then with something they have.

There are several ways that two factor authentication can be offered to the customer. It can be completed through an SMS payment security service, which sends a unique code via SMS to a customer's mobile phone to authorise online payments. Customers have already logged on to Internet banking using a password and then need to enter the SMS code before they can finalise the online payment.

Two factor authentication can also be completed through a device known as a security token which looks like a pager. It is a device issued as a credential. A token is likely to include security features that render it difficult to forge, and tying it in some manner with the particular entity – in this case the bank which issues it. To log on to Internet banking the customer uses their password and then the number generated by the token, which is then keyed in at the desktop to enable access to an Internet banking session.

Fighting cyber crime

The Australian Bankers' Association (ABA), its member banks and, State and Federal police are working closely to tackle the problem of cyber crime. Bank staff have been seconded to the Australian High Tech Crime Centre (AHTCC) as part of a new team to continue the fight against online fraud. They are providing analytical assistance to police who will use this information to identify and prosecute criminals.

Banks work closely with State, Territory and Federal police to prosecute criminals who misuse customers' personal information or commit cyber crime. Each State and Territory jurisdiction has a range of offences covering identity crime, including the unlawful possession of documents, operating accounts in false names and obtaining monies by deception. The penalties vary across each State and Territory but include large fines and incarceration, in some circumstances for up to ten years. Banks also work closely with other organisations such as the Australian Crime Commission and the anti-money laundering regulator, AUSTRAC.

Staying informed

Banks publish information about scams on their websites. The Australian Securities and Investments Commission's (ASIC) consumer website, FIDO, at www.fido.gov.au, also has lots more information about how to identify and avoid different scams and swindles.