AUSTRALIAN BANKERS' ASSOCIATION

FACT SHEET

Safety checks

Protecting your money

When dealing with banks we want you to be aware that your money is safe and secure and all personal information is handled in a confidential and safe manner. With warnings about fraud, identity theft and scams on the increase, it's only natural to be concerned. Keeping your money safe is not only about taking precautions when you bank, especially on-line – it's also about protecting your rights as a consumer. In this fact sheet, we outline these two elements and provide some important safety checks.

IDENTITY THEFT

Identity theft occurs when a dishonest individual or group gathers your personal details to make some sort of financial gain. The victim of the theft can be left with significant debt and equally significant administrative and legal problems (e.g. when someone else adopts the victim's identity to obtain accounts, licences or goods in their name).

How do they do it?

Identity thieves can obtain information in a number of ways, such as:

- theft, including theft of mail from your letterbox, or theft of your wallet;
- going through your garbage bins for discarded bills and statements;
- telephone scams;
- sending fraudulent emails which ask customers to provide their confidential Internet banking passwords or logon information;
- compromising the security of personal computers by use of trojans which are computer programs which conceal hidden programming which infects computers and are used by criminals to access or destroy other people's data.

Thieves can use your date of birth, discarded utility bills and/or your address to assume your identity.

Protecting your identity

To ensure your identity remains yours and yours alone, the following measures can help:

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. Readers should consult their own advisers on how this information may apply to their own circumstances.

- report any loss or theft of documents such as driver's licence, credit card or passport immediately;
- obtain a copy of your personal credit file (available from Baycorp Advantage - telephone 02 9464 6000, or refer to their website www.creditadvantage.com.au, (a fee may apply) at least every six months in order to check your file and make sure there have been no unexpected defaults and/or credit enquiries in your name;
- keep your tax records and other financial documents in a secure place, and don't carry identification documents (e.g. birth certificate or Medicare cards), unless you need them that day;
- close any old or unused accounts that you may have;
- secure your letterbox with a padlock if possible;
- never keep your PIN (Personal Identification Number) with your card;
- never throw away intact bills or bank statements etc. If you must discard them, shred them or tear them up to ensure that your name and address cannot be linked to any account information;
- always read your bank statements and ensure that you can account for every transaction listed.

If you fall victim to identity theft

If you are a victim of credit card fraud you may not have to pay for unauthorised transactions after the bank undertakes an investigation.

If you believe that your personal information has been used to commit a fraud, it is essential that you take the following steps immediately.

Step 1: Contact your financial institutions and any card issuers straight away – this is essential if you are to protect your accounts. You may need to stop payment of any lost or stolen cheques, change your PIN or password, or cancel your cards.

Step 2: Notify the police.

Step 3: Contact Baycorp Advantage (telephone 02 9464 6000, or refer to their website www.creditadvantage.com.au).You will need to review your credit report to ensure that no fraudulent accounts have been opened in your name. Talk to the staff at Baycorp Advantage if you need assistance. You will need to ask for all fraudulent enquires and/or defaults to be removed. As an extra precaution, request another report in a few months to ensure that it is still free of fraudulent listings.

Step 4: Check with the post office to make sure no one has requested an unauthorised change of address for your mail delivery.

Step 5: Fully document all conversations and correspondence when conducting the previous four steps (note the times, dates, names of contact people, telephone numbers and advice or information received). Keep copies of all letters sent.

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. Readers should consult their own advisers on how this information may apply to their own circumstances.

E-MAIL SCAMS AND FAKE WEBSITES

Hoax e-mails targeting bank customers are on the rise in Australia and around the world. Some of these scam e-mails look as if they've been sent to you by your bank – they even use your bank's logo.

How do they do it?

Some e-mails tell customers to update their security details and passwords by logging on to a website which, although it looks like your bank's website, is actually fake. The purpose of these websites is to obtain your logon details to access your bank accounts.

Another scam asks you to be a sales agent for a good or service, with the promise of commissions delivered to your bank account. Criminals, posing as fake companies, have been targeting consumers to act as 'money transfer agents' in the sale of goods and services through a range of means including placing hoax job advertisements, sending out unsolicited emails and approaching potential 'agents' via online chat rooms. Some customers have responded by supplying their names and banking details. These 'agents' then receive funds into their accounts along with instructions to withdraw the funds and remit them overseas. These funds are often the proceeds of fraud and people who act as 'agents' in schemes like this are effectively laundering the proceeds of crime committed against their fellow consumers.

Other types of e-mail might indicate that they contain security information or information about viruses, and advise you to install software by clicking on a link or a file contained in the email. However, by doing this, you are instead tricked into downloading a virus – some can track your every keystroke when you are logged on to the Internet, and then send the information to waiting criminals who can determine your online banking details.

Protecting your online banking

The following tips can be helpful:

- when Internet banking, always logon to your bank's website by typing their address into the address bar of your Internet browser;
- don't click on links received in e-mails;
- never respond to e-mails that request your account details and passwords (even if they look as if they are from your bank). Delete these e-mails and report them to your bank;
- don't give your account details, PINs or logon information to anyone else, and certainly never to people who telephone you and ask for the information (even if they say they are from your bank);
- change your password regularly;
- notify your bank immediately if you believe your password has been revealed to anyone;
- exit from your account as soon as you've finished your banking, and do so by following the appropriate sign-out procedures on your bank's website;
- install firewalls, anti-virus and anti-spy software on your computer and keep them up-to-date – new viruses are created every day. Learn how to use your anti-virus software to scan programs and files for viruses before you run, install or use them;

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. Readers should consult their own advisers on how this information may apply to their own circumstances.

- visit www.windowsupdate.com regularly to download security patches;
- keep up-to-date with security warnings and advices by regularly checking your bank's website;
- always check your bank statements and make sure you can account for all the transactions you see listed;
- Try to avoid using shared computers (e.g., at an Internet cafe) as you may be unable to check whether the latest anti-virus software has been installed, or take precautions when using shared computers.

PROTECTING THE RIGHTS OF CONSUMERS

Protecting your privacy

An important part of protecting your money and your accounts is protecting your privacy. Banks regularly handle money and personal details, and are bound by the Federal Government's privacy legislation to protect your privacy. You can find out more about how your bank collects, uses and stores your personal information by visiting your bank's website, or calling your bank to request a copy of their Privacy Policy.

Industry codes of practice

Many banks in Australia subscribe to the Code of Banking Practice and the Electronic Funds Transfer (EFT) Code of Conduct. These industry codes of practice set out the service standards you can expect when dealing with your bank. They help to ensure that banks have a fair process for dealing with customers and their complaints. The Codes also set out what your rights and responsibilities are and what happens if something goes wrong.

To find out more about the Codes and how they affect you as a consumer, you can access the EFT Code via the Australian Securities and Investments Commission (ASIC) website www.fido.asic.gov.au, or call ASIC directly on 1300 300 630 to request a copy.

To get a copy of the Code of Banking Practice, please contact the Australian Bankers' Association 1800 009 180 and request a hard copy or logon to the ABA website: www.bankers.asn.au and read online.

Tips for keeping your PIN secure

When a bank issues you with an access card you are usually required to select a PIN (Personal Identification Number). Avoid choosing a PIN that would be easy to guess (such as your birth date, name, telephone number or street name).

Did you know that most unauthorised transactions occur because a person gave someone else their PIN or password? Never give your PIN to another person – not even the bank will ever ask you for it. If you are telephone or Internet banking, you will be asked to enter a password and/or PIN to gain access, but your bank will never ask you to reveal your password and/or PIN.

If you can't remember your PIN, write it down and keep it somewhere safe – but never keep it in your wallet or handbag with your card (you would not want your card and your PIN falling into the wrong hands).

When entering your PIN at EFTPOS or ATM terminals, try to use your body to block the view of others as you are typing in the numbers.

Safety tips for using ATMs

Conduct your electronic transactions where you feel most secure. If you're uncomfortable withdrawing cash from an ATM at any time, try an alternative, such as using EFTPOS at a supermarket.

As soon as you've completed an ATM transaction, put your money away and leave (don't forget to take your card and a transaction receipt if you requested one). It's best to count your money later.

If you want to check your account balance or transfer funds between accounts, remember that these transactions can also be carried out over the telephone or via the Internet.

Always keep receipts of any purchases and transactions you make, and use these records to check off against your account statements.

Has your card been lost or stolen?

If your ATM or credit card is lost or stolen (or if your PIN has been revealed to another person), notify your bank immediately. This will enable your bank to put a stop on your card immediately so that no one else can use it and get access to your money. Most banks have a 24-hour telephone number for reporting lost cards – it's a good idea to keep a record of this number handy at all times, just in case. If you don't know the number, ask your bank.

August 2004

Internet: www.bankers.asn.au Phone: 02 8298 0417 Fax: 02 8298 0402

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. Readers should consult their own advisers on how this information may apply to their own circumstances.