

Protect Your Financial Identity



Identity theft involves the theft of a pre-existing identity. It may occur when a criminal steals or comes into possession of your personal information, such as your name, credit card details, address, date of birth, bank account, debit card details, driver's licence etc and assumes your identity to commit fraud. Criminals commit this crime by applying for credit, running up bills and not paying creditors – all under another person's name. Banks use a combination of safeguards to protect your information. This fact sheet prepared by the Australian Bankers' Association and the Australian High Tech Crime Centre will help you recognise the crime and also provides some useful advice on how to protect yourself from identity theft.

RECOGNISING IDENTITY THEFT

The signs can vary but some typical indicators that your identity is being used illegally are:

- A bank informs you that an application for credit was received with your name and address, which you did not apply for;
- Telephone calls or letters informing you that you have been denied credit for which you did not apply;
- You receive bank, mobile phone or credit card statements or other bills in your name, for which you did not apply;
- You notice that you no longer receive your bank or credit card statement or you notice that not all your mail is being delivered.

TIPS TO AVOID IDENTITY THEFT

If the following precautions are taken then consumers can reduce the likelihood of becoming the victim of this type of criminal activity:

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.



FACT SHEET

1. Each time you receive account statements, carefully check to ensure that they do not include any transactions that have not been initiated by you. Contact your financial institution immediately regarding any suspicious transactions.
2. Never click on a link or attachment in an email which purportedly sends you to a bank's website. Only access your bank's Internet banking logon page by typing the address into your browser.
3. If you intend destroying receipts and other personal information materials which link your name to specific account number information, ensure they are completely destroyed, so they cannot be retrieved.
4. Secure your mail by making sure your letterbox is locked and post mail at secure, official post boxes. Quickly remove mail from your letterbox after it is delivered. When you change your address, contact the financial institution and redirect your mail to the new location. If the volume of mail declines, check with the Post Office to see if anyone has filed a change of address form in your name.
5. If your credit card or other account statements are more than two weeks late you should:
 - a) Contact the financial institution and other businesses that send you accounts and confirm when and to where the statements were posted.
 - b) Contact your post office and check that someone has not redirected your mail to another address.

This emphasises the importance of being aware of your account statement cycles.

6. Protect your account information and never write down your Personal Identification Number (PIN), particularly not on your credit or debit card. To better protect your identity your PIN should be committed to memory. You must never tell your PIN or a password to anyone, including a family member or friend. Banks will never ask you for your PIN or password. When choosing a PIN do not use obvious passwords such as telephone numbers, birthdates or your mother's maiden name. Instead use passwords and PINs that will be difficult for someone else to figure out. At an ATM or EFTPOS machine, cover your hand when entering the PIN to ensure that people standing nearby cannot see the numbers you have entered.
7. Do not carry identification documents such as birth certificate, Medicare card etc, unless you need them on that day. Never carry your PIN in your wallet with an ATM card.
8. In a safe place, secure your personal information and keep a record of your account information (account number, type of account, expiry date, credit limits) and customer service contact numbers. Also keep a record of your identification documents such as passport, birth certificate, driver's licence and so on. If your wallet or purse is lost or stolen, you are then able to provide that information to the account issuers in a timely manner. Don't leave documents such as registration papers, driver's licences, utility bills or traffic fines in the car glove box.
9. Do not provide account-related information, over the telephone or on the Internet, unless you know who you are dealing with or you initiated the call. Always ask why your information is needed and how it will be used. Remember you can say no and seek further advice before disclosing any information.

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.

FACT SHEET

10. Do not respond to unsolicited emails posing as official messages from your bank.
11. When making payments by credit card or debit card, such as in restaurants or service stations, maintain a full view of the card at all times during the processing of the transaction.
12. Make sure that you fill out cheques and forms carefully so that they cannot be easily altered. Always 'cross' cheques, marking them 'not negotiable' and make sure the payee is correctly identified. When filling in forms, place a line through unused spaces.
13. Contact Baycorp Advantage to obtain your credit history report so that you are kept fully informed of any unauthorised activity on your own file. Baycorp Advantage can be contacted on (02) 9464 6000 or www.mycreditfile.com.au.

I HAVE BEEN THE VICTIM OF IDENTITY THEFT - WHAT SHOULD I DO?

If you believe that your personal information has been stolen, then you must act immediately. Once contacted, banks quickly take action – closing accounts where appropriate and commencing a fraud investigation. If the investigation proves that the customer was an innocent victim of fraud and did not contribute to the loss, banks will refund the loss.

Keep a record of all conversations and correspondence detailed in the following steps:

Action 1: Immediately contact your financial institution/s and card issuer/s so that access to your account/s can be protected. This may involve:

- Stopping payment of lost or stolen cheques;
- Changing PINs and/or passwords.

Ensure that you advise the financial institutions and card issuers of all accounts that are involved.

Action 2: Notify the police of the incident.

Action 3: Contact Baycorp Advantage on telephone (02) 9464 6000 or online at www.mycreditfile.com.au to obtain a copy of your credit history report. Upon receipt of Baycorp's report:

- Review the report to ensure that fraudulent activity has not occurred using your identity details.
- If you find fraudulent applications or overdue account listings on your report, you will need to contact the companies that have listed them so that they can investigate the matter and have the fraudulent entries removed from your credit history.
- Request a further report in a few months time to ensure that no further fraudulent activity has occurred. If there have been further entries, then carry out the same actions as detailed previously.

Baycorp Advantage and other companies provide ongoing credit monitoring services for a fee.

Action 4: Check with the Post Office to ensure that no one has requested an unauthorised change of address for your mail delivery.

Action 5: As mentioned above, fully document (time, date, contact person and telephone number, and advice received) the timing and nature of conversations in reporting the incidents to the various agencies, including the police.

TIPS FOR PROTECTING YOUR COMPUTER

It is important that you take positive steps to protect your computer if you are using e-mail, browsing websites and conducting e-commerce. Criminals try to defraud customers by use of computer programs called Trojans which monitor keystrokes, enabling the criminal to record highly privileged information such as online bank passwords and logon identification, as well as other material which is stored on your personal computer.

It is important to use only a trusted and secure computer to access your Internet banking account. Using publicly shared computers, such as those at Internet cafes, is strongly discouraged. If you use your home computer to access your Internet banking account, we recommend:

- Install reputable anti-virus and firewall protection on your computer because this provides additional layers of protection that you need to reduce your risk of exposure from viruses that can rob your computer of valuable personal information.
- Remember that after you install virus protection you will need to regularly update the software, usually by installing patches (used to update or fix a bug in a computer program) so the protection remains current.
- Install any security patches for your operating system and other software installed on your computer and keep these up to date.
- Read your bank's Internet banking security guide which can be found on the bank's website.

WHAT ARE BANKS DOING ABOUT IDENTITY THEFT?

Banks use a combination of safeguards to protect your information such as employee training, strict privacy policies, rigorous security and encryption systems. Banks have systems in place to constantly monitor online transactions. If banks come across a suspicious transaction, they will investigate it to ensure there is no breach of security. Occasionally, this may involve a bank staff member contacting you to verify a transaction. Banks will communicate with their customers regarding Internet security issues, often by publishing important information on their websites.

Some banks are working on the next step in security - two factor authentication systems. That means customers will identify themselves twice: first with something they know and then with something that they have. For example, using a password to logon to Internet banking and the bank might send an SMS message with a unique number to enter and authenticate the



FACT SHEET

transaction. This unique number could also be generated by a device known as a security token.

The Australian Bankers' Association (ABA), its member banks, State and Federal police are working closely to tackle the problem of cybercrime. Bank staff have been seconded to the Australian High Tech Crime Centre (AHTCC) as part of a new team to continue the fight against fraud that occurs online. 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 cybercrime. Each State and Territory jurisdiction has a range of offences which cover 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.

100 POINT CHECK

Checking identity when opening bank accounts is an important way of fighting money laundering and other criminal activities and this is why the law (Financial Transaction Reports Act) says that banks in Australia must identify new customers with the '100 point' check.

So, if you're opening an account for the first time, you'll need to show the bank some identity documents that prove who you are. These documents might include a birth certificate, driver's licence, passport, pensioner concession card, or even an ATM card for an account you hold with another bank. Each form of identification has a 'points' value, ranging from 25 to 100 points. Your identification documents need to add up to 100 points. To find out which documents you can use, and to make sure you've got the right documents on the day, talk to your bank and find out what you'll need.

For further information:

Organisation	Website Address
The Australian High Tech Crime Centre investigates crimes, which involve a computer or other piece of technology. It plays a significant role in reducing crimes such as hacking, denial of service (viruses, worms, Trojans), terrorism and money laundering.	www.ahtcc.gov.au
The Australian Securities and Investments Commission's consumer website FIDO has information on scams ; swindles.	http://www.fido.asic.gov.au/fido/fido.nsf

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.





FACT SHEET

The Australian Competition and Consumer Commission has a consumer protection role and their website publishes information about consumer rights.

www.accc.gov.au

State and Territory Consumer Affairs and Fair Trading - the role of these offices is to safeguard consumer rights and to advise businesses and traders on fair ethical practice.

Australian Capital Territory

www.fairtrading.act.gov.au

New South Wales

www.fairtrading.nsw.gov.au

Northern Territory

www.nt.gov.au/caft/

Queensland

www.fairtrading.qld.gov.au

South Australia

www.ocba.sa.gov.au

Tasmania

www.tas.gov.au

Victoria

www.consumer.vic.gov.au

Western Australia

www.docep.wa.gov.au

Commonwealth Attorney-General's Department Identity Fraud Prevention Kit

http://www.crimeprevention.gov.au/agd/WWW/ncpHome.nsf/Page/Publications_All_Publications_Public_Safety_ID_Theft_-_A_kit_to_prevent_and_respond_to_identity_theft

Created: February 2005

Australian Bankers' Association: Free-call 1800 009 180 www.bankers.asn.au
 Australian High Tech Crime Centre: Telephone 02 6246 2101 www.ahfcc.gov.au



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.