



Ways to Avoid Identity Fraud

Identity Fraud is a growing problem in Australia. It costs the nation up to \$4 billion a year according to the Australian Federal Police. It occurs when a criminal uses your personal information without your knowledge. These criminals can empty your bank account, buy goods using your credit card, obtain passports or a drivers licence or commit crime using your name or identity. If you become a victim of Identity Fraud, it can affect your ability to get a loan or a credit card until the situation has been resolved.

Criminals use a variety of ways to gather the information needed to steal your identity. These can range from stolen wallets, information stolen from rubbish, or stealing your identity online. All it takes is a criminal to get a hold of personal information such as your name, date of birth, mother's maiden name and address and they can open bank accounts and the like in your name. It is therefore extremely important to treat your personal information as valuable and confidential.

Moving address can pose a particular risk for Identity Fraud if the mover is not careful. It is therefore important to notify all organisations of your change of address as soon as possible. It is also wise to re-direct your mail with Australia Post to your new address in case you have missed notifying some organisations.

The **Address Change Kit** has a comprehensive package of change of address forms, contact details of notifiable organisations and information relating to changing your address. The kit also has a mail re-direction form from Australia Post. Notifying **all** organisations of your address change **quickly** will lessen the chances of future mail falling into the wrong hands.

Prevention is the best method to avoid Identity Fraud. There are some simple measures that you can take to help protect you from Identity Fraud.

The following are general tips to help avoid Identity Fraud:

- Ensure you change your address and other contact details with all notifiable organisations as soon as possible after your move. **Address Change Kits** simplify and speed this process.
- Have your mail redirected from your old address to your new address for a period of time. This form is available in the Address Change Kit.
- Consider a lock on your letterbox.
- If you are absent from your address for a period of time, have your mail held at the Post Office.
- Ensure that you destroy old credit and debit cards and sign new cards as soon as you receive them.
- Choose passwords that would be difficult for someone to guess, as birthdays and pet names can be easily discovered and used. Change them regularly and if you do need to write them down, make sure they are stored in a secure place or 'in code'. Do not store them in your wallet or bag.
- Check that you have received your bills and statements on time. A missing statement/letter could indicate that a criminal has changed your billing address.
- Keep all your receipts and check any account statements for any discrepancies.
- Shred or destroy any records/statements/bills that contain personal information before you put them in a bin. It is far too easy for criminals to get vital information from these records if they are just placed in a bin.
- Don't give out personal information over the phone or by email if you haven't been the one to make the initial contact.
- Do not use the same signature that you would use for a legal document or to verify your bank account signature when you sign for everyday things. For example, you are sending a parcel to someone who has bought an item from you through eBay. You will have to sign the Australia Post pack if sending

interstate. Ensure that this signature is different to your 'legal' signature. Your signature in the wrong hands could be a big problem.

- When paying for goods over the internet, make sure that the site you are using is safe and secure. Look for the padlock sign, 'https' in the address, or other secure signs that indicate the site is safe.
- Ensure that you have up-to-date antivirus software installed and the latest security patches.
- You may receive an email from an organisation that requests you to open their web site from the sent email. Make it a rule never to click on a web site link from an email. Criminals use this technique called 'phishing' to obtain either your account details or passwords. These emails may look very authentic and can appear to be from a major bank or other organisation. Always type in the correct, known web address of the bank or organisation yourself and check to see if there is a message attached to your account that confirms the email. You can also ring the organisation to ask if the email sent is legitimate. Report it if it is not. I was caught early days with a bogus eBay email that claimed I had not paid for an item. My immediate reaction was "That can't be right, I have to check this out!" and so I clicked on the web link in the email and continued to enter my log in and password. I was unaware of what I had done until the real 'eBay' contacted me to tell me to change my password as it had been compromised.
- Photocopy and/or list all your credit cards, debit cards, bank and investment account numbers, passport, and other cards that are in your wallet. Also have a list of contact details of organisations that you would have to contact if your wallet or identity were stolen. Keep these photocopies in a safe, secure place. A list of emergency contact details is included with this Fact Sheet.
- If you own a cheque book, ask the bank to only print your initials on the face of each cheque. Then if someone steals your cheque book, the thief will not know your full name and can not 'guess' how to sign your name.
- For extra protection, do not sign the back of your credit cards. Either opt for the password option or write 'Photo ID required' on the back of the credit card.
- Don't write your home address or phone number on your cheques. Use a work number or address or a PO Box address.
- Don't allow your credit card to be taken away from you for processing. Your card could be scanned for its data on the magnetic side into a device no larger than a calculator, for later processing of fraud cards.

What to do if your details/wallet has been stolen:

- Contact all organisations where you have cards or accounts that could have been compromised. Have your card numbers handy (from the photocopies of your cards as outlined in the tips above). Refer to the phone numbers below of organisations you may have to contact.
- Immediately report the problem/theft to the local Police office where the theft took place.
- Most importantly, immediately contact the three national Credit Reporting organisations to inform them of the incident and to request a file note or fraud alert on your file. This alert means that any company that checks your credit will know that there is a potential problem and will have to contact you by phone to authorise any new credit. This simple measure can very effectively stop the criminals from obtaining credit in your name. You can check your credit file for any accounts that have been opened in your name or any changes made to your account. If you discover fraudulent activity on your report, contact the organisations involved to investigate the incident and have the fraudulent activity removed from your credit history. Check your credit files and other financial records in the months after the criminal activity, then every 3 months in the first year. Check yearly after this.
- Ensure that you write down all the details regarding the conversations you have with the organisations above including the police. This should include the date, time, person's name, phone number and information from the phone call.
- Check with your Post Office to see if any of your mail has been re-directed to another address.
- Check with all Government Departments that may need to be informed of the fraudulent activity. This could include the Australian Passport office, Transport Department and Centrelink.

NOTE: This fact sheet is for information purposes only and should not be relied upon as legal advice.

Important Contact Details

3 Main Credit Reporting Agencies

1. Veda Advantage, previously known as Baycorp Advantage – 1300 762 207 or 13 31 24, www.mycreditfile.com.au

2. Dun & Bradstreet (Australia) Pty Ltd – 13 23 33, www.dnb.com.au

3. Tasmanian Collection Service (for Tasmanian residents) – (03) 6213 5555, www.tascol.com.au

State Police Contacts:

QLD Police – (07) 3364 6464

NSW Police - 131 444

VIC Police – (03) 9247 6666

WA Police - 131 444

SA Police - 131 444

TAS Police – (03) 6230 2111

ACT Police – (02) 6256 7777

NT Police - 131 444

Other Contacts:

Crime Stoppers - 1800 333 000

mainland Australia, 1800 005 555 Tas.

Centrelink – fraud tip off line - 13 15 24

The Australian Taxation Office ATO -

1800 060 062, www.ato.gov.au

The Australian Securities and Investments Commission (ASIC) -

1300 300 630

Medicare – 132 011

Seniors Card – 1300 364 758

Banks & Credit Cards

Commonwealth Bank – 132 221

ANZ – Freecall 1800 033 844 or 133 333

Westpac – 1800 230 144 or 132 032

National – 132 265

St George – 1800 028 208 or 133 330

Macquarie Bank – (02) 8232 3333

BankWest – 131 718

Citibank – 132 484

ING Bank – 131 688

ING Direct – 133 464

Suncorp – 131

AMP Banking – 133 030

HSBC – 1300 308 008

Woolworths Ezy Banking – 137 288

Bank of QLD – 1300 557 272

Bendigo Bank – 1300 366 666

Adelaide Bank – 132 220 (within SA),
- 1300 652 220 (outside SA)

MasterCard Australia - (02) 9466 3700

MasterCard International 1800 120 113

Visa Card Australia – 1800 621 199

Visa Card International – 1800 450 346

Travellers Cheques lost – 1800 127 477

ORDER YOUR [Address Change](#) KIT NOW!

(the most complete address change package available, tailored to your state)