



An Australian Government Initiative

id Theft

A kit to prevent and respond to **identity theft**

Acknowledgements

The National Crime Prevention Program – Towards A Safer Australia, would like to acknowledge the following organisations for their contribution to the development of this kit:

- Australian Institute of Criminology
- Australian Federal Police
- Australian Crime Commission
- Australasian Centre for Policing Research
- Office of the Federal Privacy Commissioner
- Australian Taxation Office
- Australian Securities and Investments Commission
- Department of Foreign Affairs and Trade
- Department of Immigration, Multicultural and Indigenous Affairs
- Insolvency and Trustee Service Australia
- Centrelink
- Design: Design Direction
- Printing: Union Offset Printers
- Photography: www.geoffcomfort.com

dealing with identity theft

A message from the minister



An individual's identity is a personal part of who they are. Having their identity stolen can have a devastating effect, both emotionally and financially. Victims can often spend years and thousands of dollars trying to restore their good names.

The risk of becoming a victim of identity theft in Australia is still relatively small. However it is important that we recognise the increasing threat this poses to us all, as a nation and individually. It is important that we take steps now to prevent identity theft.

By introducing some practical precautions into everyday life, you can take an active role in reducing the risk that your identity may be used without your consent or knowledge. There are also a number of steps you can take to recover your good name and limit the damage done if you are an unfortunate victim of this crime.

The Australian Government, through its National Crime Prevention Program, is committed to helping all Australians protect themselves and their families in an effort to reduce the likelihood of becoming a victim of identity theft.

In addition, the Australian Government is working in partnership with state, territory and international governments, and with the business and finance sectors, to develop strategies to prevent and respond to identity fraud and identity theft related issues.

Simple steps you can take to minimise your risk of becoming a victim of identity theft include:

- Destroy all identifying information when disposing of personal papers, including bank statements, utility bills, such as phone, electricity and gas bills.
- Don't give out personal information over the phone or by e-mail unless you have initiated the contact or are confident the caller is who they claim to be.
- Check accounts and other records carefully. Know when accounts are due. A late or missing account could mean a billing address has been changed and your identity has possibly been stolen.
- Use a separate bank account with a low credit limit for internet transactions.

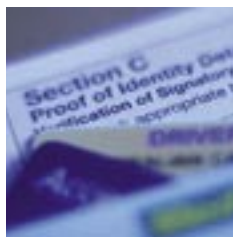
This kit, 'How to prevent and respond to identity theft' contains useful information to help you identify where you might be vulnerable, and what to do, to avoid becoming an identity theft victim.

I would encourage you to use the kit and to share it with friends and relatives to help prevent identity theft.

A handwritten signature in black ink, reading "Chris Ellison". The signature is written in a cursive, flowing style.

Senator Chris Ellison
Minister for Justice and Customs
Senator for Western Australia

Identity theft



Identity theft - what is it?

Identity theft is part of identity fraud and specifically refers to the theft and use of personal identifying information of an actual person, as opposed to the use of a fictitious identity. This can include the theft and use of identifying personal information of persons either living or dead.

Identity fraud

The cost of fraud is increasing both in Australia and internationally. It can be devastating to both business and individuals. But what is fraud? Basically, fraud is gaining a benefit by deception. Usually, but not always, such gains are financial.

Being able to prove who you are is an important part of modern life. You often have to identify yourself to receive services and conduct normal everyday transactions—making a purchase, paying a bill, using your credit card, seeing the doctor or driving your car. In particular, most government and business organisations have procedures to establish the identity of new clients when entering into transactions for the first time.

Normal transactions involve only two parties—you and the supplier. Identity fraud normally occurs when a third party uses deception to get a benefit. Identity thieves can appear like a legitimate customer and ‘pass’ the procedures and tests that businesses and organisations use to verify clients’ identities. This breach of procedure usually occurs in one of these ways:

- the creation and use of an entirely new ‘fictitious identity’ for fraudulent purposes
- the unauthorised use of a ‘stolen identity’ of a real person to gain a benefit.

Identity theft—how can it happen?

Identity theft happens in a multitude of ways. It can range from somebody using your credit card details illegally to make purchases over the internet or telephone, through to having your entire identity assumed by another person to open bank accounts, take out loans, make tax returns and conduct other business illegally in your name.

Identity theft can happen easily. Most often you will not even know you are a victim until well after the fact. It can happen quickly. You might have your credit card details skimmed when you make a purchase, lose your wallet or other personal effects, or have them



stolen. You could inadvertently provide your details by phone or email to what you think are legitimate businesses or have your personal information stolen from an unsecured site on the internet. Perhaps most unexpected of all, you could have your identity stolen and used by someone you know and trust—a friend, relative or work colleague.

Identity fraud – what does it cost Australia?

With the rise and spread of globalisation, identity fraud has become one of the fastest growing crimes in the world. The rapid development of new technologies, telecommunications and internet access, and the growth in trade and the deregulation of financial markets have extended the reach of international fraudsters and challenged the traditional boundaries between nations.

Globally, false and stolen identities are being used in an expanding range of criminal and terrorist activities. The cost of identity fraud in Australia has been estimated at \$1.1 billion for 2001-02. However, this figure does not take into account the non-financial costs to organisations or victims, nor the amount of undetected identity fraud. Other research indicates that if these measures were taken into account, the figure would be much higher.

Desperation in the US

US federal courts are dealing with a range of cases of identity theft, such is the desperation of these criminals.

In one case, an offender allegedly murdered a homeless man so that he could fake his own death and avoid prosecution for counterfeiting.

In another case, a hospital employee allegedly stole 393 hospital patients' identities to obtain credit card details.

Bizarre as these US cases seem, we should not be complacent in Australia.

(Rusch 2002, p.1)

Both government and private sector agencies in Australia are beginning to acknowledge the threat that identity related fraud poses to our way of life. Currently, there are few statistics on the incidence of identity fraud in Australia. However, it is likely that Australia will follow international trends. For example, in 2000 the FBI estimated that up to half a million¹ instances of identity theft occur in the United States each year, and that figure is growing.

Whilst all reasonable care has been taken in the preparation of this information sheet, no liability is assumed by the Commonwealth of Australia for any errors or omissions.

1 Congressional Press Release, 12 September 2000.

How your identity may be stolen

How does a thief get your personal information?



Despite your best efforts, a determined thief may still be able to access your personal information. Here are some ways this can happen:

- Your wallet or purse contains personal information such as your licence, credit and ATM cards, Medicare card and other personal documents, that may be stolen.
- Your home is burgled and your personal information and documents, or those of close family members, may be taken.
- Many important documents are posted to you and can be stolen from your letterbox. For example, bank and credit card statements, new cheque books, ATM and credit cards, taxation returns or cheques, or pre-approved credit card offers. You may be unaware that these were sent to you if they do not arrive.
- Your mail may be diverted to another address. It is simple for a thief to use a false identity and fill in a 'change of address' form.
- Your rubbish (or that of businesses you have dealt with) may be searched. Information found in the garbage could provide a thief with a head start in stealing your identity.

How identity thieves work in Australia

One Melbourne offender obtained the birth certificates of four babies who had died in the 1970s and then, over eight months, claimed \$20,857 in unemployment benefits in their names.

When arrested, the offender had with him a bag full of false Proof of Identity documents to support his welfare claims. These included motor vehicle learner's permits, mobile phone accounts, student cards, rental documents and bank account access cards.

(Protyniak 2000 cited in Ringin 2001, p.6)

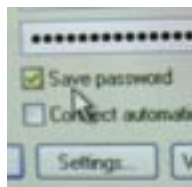


- You may be the victim of a scam and be conned into providing personal information over the telephone or by email.
- Your personal computer may be hacked into, or hackers may get into the computers of businesses that hold your personal information.
- Your ATM or EFTPOS transactions may be monitored by hidden devices or seen by the person next in the queue. Your password or PIN may be noted for subsequent unauthorised use.
- Your personal information may be stolen and used or sold by employees of legitimate businesses: for example, credit card skimming at retail outlets or restaurants (Credit card skimming occurs when your credit or EFTPOS cards are secretly 'skimmed' with a small device that copies the information on the card's magnetic strip. Your information can then be transferred to a blank credit card to be used without your knowledge. For example, card skimming may occur by use of a small hand held device by staff in retail outlets such as restaurants or petrol stations, or by criminals inserting a small hidden device in the card slot of EFTPOS or ATM outlets).



Preventing identity theft

What can you do to stop identity theft?



Everyday, you engage in transactions that require the sharing of personal information. You may share personal details when you pay bills, make purchases, pay taxes, rent accommodation, open bank accounts, order new cheques or credit cards, register a car, get insured, rent a video or log on to a computer.

To complete these transactions, you often provide information such as your name, address, phone number, driver's licence number, or sometimes even bank account or credit card numbers, and tax file number. Elements of your personal information exist in every business or organisation with whom you have ever conducted a transaction.

Often large amounts of information are requested from you which the business doesn't really need. You should aim to provide the minimum of information about yourself, and if the request for information seems inappropriate, ask why it is needed.

While it may never be possible to stop identity theft entirely, there are a number of very simple safeguards you can take to protect yourself from becoming a victim of this type of crime.

- **Order a copy of your credit report regularly.** Your credit report contains important information about you and your credit history. It also contains information on most credit applications made in your name. By checking your own credit report regularly you can often catch any unauthorised activity. Such activity may indicate that your identity has been stolen. There are three main credit reporting agencies in Australia. These are Baycorp Advantage, Dun and Bradstreet, and the Tasmanian Collection Service. You will find contact details in this kit.
- **Place passwords on all your important accounts.** Passwords help provide extra protection to important information such as credit card and bank accounts, phone and other utility accounts. Avoid using obvious passwords such as telephone numbers, birth dates or your mother's maiden name. Instead use passwords and PINs that will be difficult for someone else to figure out. Don't use the same password on different accounts, such as bank, video card, internet service provider. Be careful of writing your passwords down or storing them on your computer.



- **Secure your personal information.** If possible, secure all personal information at home in a lockable filing cabinet or safe. If you share accommodation or have maintenance or cleaning services in or around your home regularly, having a secure place for such documents is particularly important. Collect new cheque books or credit cards in person from the bank. Don't leave documents such as registration papers, driver's licences, utility bills or traffic fines in the car glove box. Don't lend your personal documents to others. Once they are out of your control, you cannot be sure how they are used.

- **Don't carry personal information unless you have to.** Unless you really need to, do not carry important documents around with you outside your home. Never carry your PIN in your wallet with the ATM card. When you leave the house, carry only the ATM and credit cards you need. Don't carry documents like your passport or birth certificate unless you have to. Be wary of people acting suspiciously at ATMs, and avoid using ATM or EFTPOS facilities that look as if they have been tampered with.

- **Destroy personal information before disposal.** Before placing old bills, records or expired cards in the rubbish ensure that any identifying information is destroyed. If you get a pre-approved credit card and you don't want to accept or activate that card, make sure you destroy identifying information before throwing it away. This can be done in the same way as you should destroy all old records, files, bills, expired credit cards or other cards—by tearing, cutting up, or burning them before throwing them in the rubbish. Home shredders can be a good investment.

- **Avoid giving personal information out over the phone, by mail or on the internet.** Make sure you know who you are dealing with before you give out personal information. Only provide the minimum information necessary to those with whom **you** have initiated contact or whom you have checked independently. Always ask why your information is needed and how it is going to be used. Don't be afraid to say NO or seek further advice before disclosing anything. Be suspicious when things don't seem right. Unsolicited offers that seem too good to be true or that require you to give out bank account or other personal information are likely to be scams.

- **Secure your mail.** Make sure you have a secure lockable letterbox and only post mail at secure, official post boxes. Make sure your letterbox is large enough to accept and hold mail in the quantity and size you normally get. Quickly remove mail from your mailbox after it is delivered. If you are going away, have it held at the post office. If the volume of mail drops off substantially, check with the post office to see if anyone has filed a change of address form in your name.



- **Check your billing and account records carefully.** By carefully checking all transactions on your banking and credit card accounts you may be able to detect potential identity theft early. Follow up if your bills or accounts don't arrive on time. Missing records or accounts could indicate that your accounts have been taken by a thief who has changed your billing address.
- **Limit the amount of credit you have in accounts.** For certain transactions, such as those made by telephone or on the internet, it is best to use a separate account with a low credit limit, so that if the account is misused, the loss will be minimised.
- **Write cheques and fill out forms carefully.** Make sure that you fill out cheques and forms carefully so that they cannot be altered easily. Always 'cross' cheques and mark them 'not negotiable' and make sure that the payee is correctly identified. In cheques and other forms put a line through unused spaces.



Proof of identity

The use of false or stolen identities provides a means of committing fraud, terrorist acts, illegal immigration as well as posing a threat to electronic commerce.

Work to address identity fraud is being undertaken across many government agencies and the Australian Government is undertaking a whole-of-government strategy to reduce the incidence of identity fraud and financial crime in Australia. This strategy is being developed in partnership with State and Territory Governments and is aimed at enhancing identification and verification processes as well as identifying other measures to tackle this important issue. Other Australian Government initiatives include:

- A national response to credit card skimming
- The ACC's trial Identity Fraud Register which records known offenders, fraudulent names used, and lost or stolen documents
- Introduction of world's leading identification technology to combat passport fraud
- Establishing an ID Taskforce chaired by the Australian Federal Police to investigate identity-related crime.

- **What if your wallet, purse or credit cards are lost or stolen?** Contact your bank or credit provider immediately and cancel all cards and freeze all accounts to which the thief may have gained access. Make sure you have some way of accessing cash for the time it will take to get new cards issued. Make sure you ask that all new cards and account numbers are issued with new Personal Identification Numbers (PINs). It is also important that you report the theft or loss to the police. Your identification could be used to commit other criminal offences.

- **List all your account details.** Keep a list of all your accounts and credit cards in a safe place. Also make a list of contact numbers in case those account details are stolen, or if you lose your wallet or purse. It is important to act quickly if personal information is compromised.
- **Remove your name from mailing lists.** If you receive mail addressed to you from companies you have not had any dealings with, or receive pre-approved credit cards that you did not apply for, do not just throw these in the rubbish and forget about them. Contact the company or credit provider making the offer and ask that your name be removed from any further mailing lists. It is particularly important to take this action if you are unexpectedly offered a pre-approved credit card.

Using computers securely

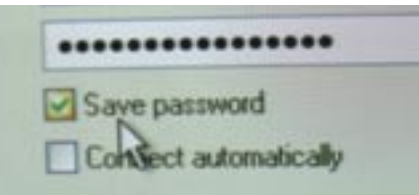
How to use your personal computer securely



More and more people use computers and the internet to communicate, store information, and conduct business. Your computer could be your weakest link in preventing theft of your identity. All kinds of important personal information may be stored on your computer, including tax records, birth dates and financial records. When you access the internet to do business such as banking

or making a purchase on-line, your PIN, banking details or credit card numbers may be left on the hard drive of the computer you have used. With today's technology, an identity thief can obtain this private information without setting foot in your house. If you follow a few simple steps you can make identity theft via your PC more difficult.

- **Use passwords.** Passwords help provide extra protection to important information stored on your computer. Avoid using obvious passwords, such as telephone numbers, birth dates or your mother's maiden name. Use passwords that will be hard to guess, such as a combination of letters, numbers and symbols.
- **Update your password.** Regularly change the password on your PC and laptop. Remember to use a combination of numbers and letters. You may wish to consider using encryption software. DO NOT use automatic log in features that save your user name and password. Always remember to log off. Avoid saving important personal data (especially financial data) on your computer—save it to a floppy disk and keep the disk secure. If your computer is stolen, taking these precautions will make it harder for the thief to access your information. Consider buying a program that will ask you to change your password regularly and will shut down your computer after a set time.
- **Use the latest protection software.** Regularly update your protection software such as virus protection programs and encryption browser programs to protect your computer from viruses on disk or CD, sent to you via e-mail, or that you inadvertently download from the internet.
- **Use a personal firewall to secure your PC when online.** A firewall will stop unauthorised access to your computer. Firewall programs are particularly important if you use a high-speed internet connection and leave your computer connected 24 hours a day. Many firewall programs are available free of charge on the internet.





- **Beware of unsolicited e-mails.** Do not open files or click on links sent to you from people you do not know. These may contain viruses or other programs that can access information on your PC. Unsolicited e-mails are also used to promote scams: do not follow the advice of e-mails from sources you do not know, especially ones that ask you to give out personal information or induce you to part with your hard-earned cash. Criminals have been known to send messages in which they pretend to be representatives of legitimate organisations, such as banks or your ISP, in order to persuade people to disclose important personal information.
- **Do not follow up unsolicited e-mails.** If you receive unsolicited emails, don't reply to them requesting your name to be removed from the mailing list. This often simply confirms that your address works and that you exist. Simply delete the e-mail and remove it from your deleted file storage. You should also delete any attachments from other folders in which they are stored (ask your computer shop how to do this if you don't know).
- **Only conduct transactions with secure websites.** If you do business with companies on-line, ensure each site contains a statement about the company's privacy policy with which you are comfortable. The policy should include details on how the company will secure, handle and use your personal information. It should also tell you how to contact the company and how to provide personal information without using the internet. A good indication of a secure site is the presence of the small padlock symbol. If a company with whom you intend doing on-line business does not have such a policy, or you do not agree with their information handling practices, consider looking elsewhere.
- **Wipe your hard drive.** Before you dispose of, sell or trade in your old PC or laptop, be sure you have deleted all personal information properly. Deleting files using the keyboard delete key or mouse may not be enough. All files, including e-mails, may still be on your hard drive where they are easily retrieved. Use a program that 'wipes' your entire hard drive and makes all files unrecoverable.

Identity crime and technology

The explosion of identity crime has been linked to the development of technology. In particular, it is linked to the easy access we now have to desktop scanning and publishing programs for our computers, and to internet access.

By September 2001, 67 per cent of Australian households owned or leased a computer, and 54 per cent had internet access.

This rate of usage will increase, and as more government and other large organisations come online, more opportunities will be presented to criminals to commit identity crime.

(National Office for the Information Economy 2002)

- **Don't use public computers to access your private information.** Be wary when accessing your private information, particularly financial records, on public computers at libraries or internet cafés. Passwords, credit card and account numbers may be retrievable from the hard drive of the computer you have used and accessible to anyone with the 'know how'.

Note: PC and 'personal computer' mean any computer in your personal control, regardless of brand or size, and includes laptops.

Whilst all reasonable care has been taken in the preparation of this information sheet, no liability is assumed by the Commonwealth of Australia for any errors or omissions.

When identity thieves strike

What to do if you become a victim of identity theft



Unlike other crimes, victims of identity theft may not know they are victims until weeks or months after the theft has occurred. Often the first indication that your identity has been stolen is when you have an application for credit refused, you are notified you have defaulted on a loan you did not apply for, or worse yet you are arrested for a crime you did not commit! However, what you do when you realise you are a victim of identity theft can minimise the damage to your good name and prevent further crimes being committed.

- **Report to the Police.** Like any other theft, incidents of identity theft should be immediately reported to the police even if only small sums are involved, as they can provide a profile on how the fraudster has operated. Assist the police by providing relevant documentation so they can record and follow up your case. Your credit report, account statements, debt collection letters and other evidence of fraudulent activity using your identity can greatly assist police. Ask for a copy of the police report—sometimes banks or other financial institutions will ask you for a copy.
- **Contact the Credit Reporting Agency.** Inform the credit reporting agency that you are a victim of identity theft. Ask that an alert be placed on your file that advises this. You have the right to include a written statement on your file. In your statement, ask that credit providers contact you (by telephone) before they open any new accounts for you or change any of your existing accounts. This way, additional fraudulent accounts being opened in your name should be avoided. The credit agency should send you a copy of your new credit file with these revisions. It should advise you of your right to have organisations who have accessed your file in the past three months informed of these changes. You should ask when this will happen. You should not be charged to access your file. If you are told you cannot access your own file because you refuse to pay the fee, seek advice from the Federal Privacy Commissioner. (www.privacy.gov.au)
- **Review your credit file carefully.** You need to check your credit report carefully. Look for any accounts that you did not open or where any unauthorised changes have been made to your existing accounts. Ensure you can authenticate all 'enquiries' made into your credit history. Note the companies and organisations that have either made inquiries or opened accounts under your name that you did not authorise.

- **Close all accounts and correct your credit file.** Contact the credit providers and businesses with whom any unauthorised accounts have been opened in your name, or who have made enquiries about your credit file. Remember this includes phone and other utility providers and department stores as well as financial institutions. Inform them, and the credit reporting agencies, that you have been a victim of identity theft. Ask credit providers to close the fraudulent accounts and to tell the relevant credit reporting agencies to remove references to the accounts and enquiries from your credit file. Usually, the credit provider will need to conduct an investigation to establish that you are not responsible for any debts that have been incurred in these accounts and you may have to supply additional documentation. Where there is a large number of credit providers involved, it may be impractical to deal with each one individually. In this case, contact the credit reporting agency first on how best to remove the incorrect entries. You may also want to close any legitimate accounts you hold so that these cannot be tampered with in the future. Replace them with new accounts, with new PINs and passwords.
- **Keep all documentation.** Take notes that include dates, names, contact details and what was said. Follow up all conversations and requests in writing, and send these certified mail if you need to post them. Keep copies of all forms and correspondence. Keep all original supporting documents, such as the police report, letters, and your credit file—never put originals in the post. Ask all agencies that you speak to, including banks and other financial institutions, to write to you confirming the actions they have taken or will be taking and when they expect to complete such action. Ask them to provide details of all accounts in your name that have been closed and ensure that they acknowledge that you are not responsible for any further debts incurred. Keep a record of how much time you have spent on this and receipts for how much you have spent on copying, postage, etc, as you may be able to claim these costs back.



- **Clearing criminal records.** Take action to remove any criminal records, arrest warrants or traffic infringements issued against your name as a result of the theft. The police will probably be your first point of contact. They may need to take your photograph and/or fingerprints to establish that your identity is different from that of the person charged. Ask that your name be removed from the offenders' database and noted as an 'alias' only. Hire a lawyer if you need help to clear your name. Contact Legal Aid or the Law Society in your state or territory for more information.

- **Specific fraud offences.** Contact the relevant government agencies if you think your identity may have been used for other fraudulent activities, including:

- passport fraud
- taxation fraud
- business fraud
- visa and immigration fraud
- welfare fraud
- bankruptcy fraud.



You'll find contact details in this kit.

Whilst all reasonable care has been taken in the preparation of this information sheet, no liability is assumed by the Commonwealth of Australia for any errors or omissions.

Important contacts

The Australian Crime Commission

The Australian Crime Commission operates an Identity Fraud intelligence facility that can assist victims in notifying some Australian and State government agencies that their identity has been stolen.

Tel: (02) 6243-5666

Australian Federal Police

The Australian Federal Police (AFP) is the Commonwealth's primary law enforcement agency and the chief source of advice to the Australian Government on policing issues. Its role is to enforce Commonwealth criminal law and protect commonwealth and national interests from crime in Australia and overseas. The AFP is also Australia's international law enforcement and policing representative.

For operational policing, the AFP provides national leadership as a member of the Identity Crime Taskforce, which comprises members drawn from a number of Australian and State Government agencies.

Tel: (02) 6256 7777

– National Headquarters (Canberra)

Website: www.afp.gov.au

In the first instance, identity theft should be reported to your local State or Territory police.

Australian High Tech Crime Centre

The role of the Australian High Tech Crime Centre is to provide a national coordinated approach to combating serious, complex and/or multi-jurisdictional high tech crimes.

If you believe that your identity has been compromised through complex scams on the internet (such as false banking or other e-commerce websites), or the use of malicious software (such as viruses) to compromise your home or business computer, please use the on-line crime reporting facility.

Website: www.ahtcc.gov.au

Tel: (02) 6246 2101

Crime Stoppers

Crime Stoppers is a community based reporting mechanism to assist the police to respond to crime. Crime Stoppers allows the community to effectively participate in the fight against crime. By calling Crime Stoppers you can report crime anonymously with no questions asked. If you would like to report an identity theft or identity related crime, you can contact Crime Stoppers on:

Tel: 1800 333 000 – Mainland Australia,
or 1800 005 555 – Tasmania.

Website: www.crimestoppers.com.au

Credit Reporting Agencies

Three major credit reporting agencies in Australia provide information on your credit history to credit providers and businesses. These agencies maintain a file on the credit accounts applied for or opened in your name. You are entitled to access your own credit file. If you find fraudulent activity on your credit file, you can prevent possible further misuse of your identity.

- **Baycorp Advantage**
Public Access Division
Credit Reference Association of Australia
PO Box 966
NORTH SYDNEY NSW 2060

Tel: Public Enquiries: (02) 9464 6000
Fax: (02) 9951 7880
Email: assist.au@baycorpadvantage.com
Australia website:
www.baycorpadvantage.com
- **Dun and Bradstreet (Australia) Pty Ltd**
Attention: Public Access Centre
PO Box 7405
St Kilda Rd VIC 3004

Tel: 13 23 33
Australia website: www.dnb.com.au
- **Tasmanian Collection Service** for
Tasmanian residents
Box 814H Hobart 7001 or
Box 525F Launceston 7250 or
Box 241 Devonport 7310 or
Box 355 Burnie 7320

You can also contact the Tasmanian
Collection Service on
Tel: (03) 6223 5599

Federal Privacy Commissioner

Access to and management of personal information, including that contained on your credit file is governed by the *Federal Privacy Act 1988*, and the Act is enforced by the Office of the Federal Privacy Commissioner. View their website if you want to find out more about your privacy rights, or contact the hotline if you want to make a specific enquiry or lodge a complaint against a credit agency.

Office of the Federal Privacy
Commissioner
GPO Box 5218
Sydney NSW 2001

Privacy Hotline: 1300 363 992
Fax: (02) 9284 9666
Email: privacy@privacy.gov.au
Website: www.privacy.gov.au

Australian Taxation Office (ATO)

The ATO collects revenue for the Australian Government, and maintains the tax file number system. If you believe your identity or tax file number has been used to commit taxation fraud and/or welfare fraud, contact the ATO on:

Tel: 13 28 61
Website: www.ato.gov.au

Australian Securities and Investments Commission (ASIC)

The Australian Securities and Investments Commission (ASIC) maintains Australia's public database of 1.3 million companies. They register new companies, record changes in structure and ownership of ongoing companies, and deregister defunct companies. If you suspect your identity has been fraudulently used in the creation or amendment of a company record, contact ASIC on:

Tel: 1300 300 630
Email: infoline@asic.gov.au
Website: www.asic.gov.au

Department of Foreign Affairs and Trade (DFAT)

DFAT's role is to advance the interests of Australia and Australians internationally, including the approval and issue of passports for Australian citizens, subject to the provisions of the Passports Act 1938 and other relevant legislation. If your passport is stolen (or lost) or if you believe that your identity has been used to commit passport fraud, contact DFAT on:

Tel: 131 232 (if your passport is lost or stolen within Australia)

If your passport is lost or stolen whilst you are overseas, report to the nearest Australian diplomatic or consular mission.

Website: www.passports.gov.au

Department of Immigration, Multicultural and Indigenous Affairs (DIMIA)

As its name implies, DIMIA is a department with a variety of roles. Of particular importance to the issue of identity theft, DIMIA is responsible for the provision of services for persons who are either migrating to Australia or visiting from overseas. This includes responsibility for the issuing of visas for people wishing to come to Australia on either a permanent or temporary basis. If you believe your identity may have been used illegally by someone to enter Australia, contact DIMIA on:

Tel: 13 18 81

Website: www.dimia.gov.au

Centrelink

Centrelink is an Australian Government agency delivering a range of services to the Australian community. Most people getting payments from Centrelink are in genuine need. However, there are people who don't provide Centrelink with the correct details of their personal circumstances (or a change in

circumstances) which they are obliged to disclose. Centrelink carries out a range of regular reviews to make sure the right customer is paid the right amount. If you believe your identity may have been used illegally by someone to obtain a payment they are not entitled to, contact Centrelink.

- Report a suspected fraud online at www.centrelink.gov.au;
- Telephone the Centrelink Report a Fraud line on 13 7230;

Insolvency and Trustee Service Australia (ITSA)

ITSA is an agency within the portfolio of the Australian Government Attorney-General's Department, responsible for personal bankruptcy and insolvency law. If you suspect your identity has been used to commit bankruptcy fraud, write to ITSA at:

Website: www.itsa.gov.au or

(For NSW and Queensland)

ITSA Fraud Investigations

Level 13

340 Adelaide Street

BRISBANE QLD 4000

or PO Box 10443, Adelaide Street

BRISBANE QLD 4000

(For all other states and territories)

ITSA Fraud Investigations

Level 10, Melbourne Central

360 Elizabeth Street

MELBOURNE VIC 3000

Defence Signals Directorate (DSD)

DSD is the Australian Government's national authority on information security. It regularly evaluates the security of computer products and provides a list of evaluated products.

Website: www.dsd.gov.au

Identity fraud information and assistance sites

Further information is available from these Websites:

Australian Government Agencies

- Australian Institute of Criminology (<http://www.aic.gov.au>)
- Australian Competition and Consumer Commission (<http://www.accc.gov.au>)
- Consumers Online (<http://www.consumersonline.gov.au>)
- Consumer Affairs Division – Department of the Treasury (<http://www.ecommerce.treasury.gov.au/>)
- Ministerial Council on Consumer Affairs (<http://www.consumer.gov.au/>)
- Net Alert (<http://www.netaalert.net.au>)
- Australasian Centre for Policing Research (<http://acpr.gov.au>)

State Agencies

- South Australia Police (<http://www.sapolice.sa.gov.au/>)
- New South Wales Police (<http://www.police.nsw.gov.au/>)
- Victoria Police (<http://www.police.vic.gov.au/>)
- Queensland Police (<http://www.police.qld.gov.au/>)
- Tasmania Police (<http://www.police.tas.gov.au/>)
- Northern Territory Police (<http://www.nt.gov.au/pfes/>)

- Western Australia Police (<http://www.police.wa.gov.au/>)
- Crime Prevention Victoria (<http://www.justice.vic.gov.au/>)
- NSW Crime Prevention Division (<http://www.lawlink.nsw.gov.au/cpd.nsf/pages/index/>)
- SA Crime Prevention Unit (<http://www.cpu.sa.gov.au/>)
- Crime Prevention Queensland (<http://www.premiers.qld.gov.au/about/crimeprevention/index.htm>)
- NT Office of Crime Prevention (<http://www.crimeprevention.nt.gov.au/>)
- Victoria Consumer and Business Affairs (<http://www.consumer.vic.gov.au/>)
- Queensland Office of Fair Trading (<http://www.consumer.qld.gov.au/>)
- Tasmanian Office of Consumer Affairs and Fair Trading (<http://www.justice.tas.gov.au/ca>)
- WA Electronic Commerce Centre – Fair Trading (<http://www.ecc.online.wa.gov.au/matrix/legal-fair.htm>)
- NSW Office of Fair Trading (<http://www.fairtrading.nsw.gov.au/>)

Private Organisations

- Australian Bankers Association (<http://www.bankers.asn.au>)
- Macquarie Bank (<http://www.macquarie.com.au>)
- Australian Consumers Association (<http://www.aca.com.au/>)

International Sites

- Office of Fair Trading (UK) (<http://www.oft.gov.uk>)
- Federal Trade Commission (USA) (<http://www.ftc.gov>)
- United States Department of Justice (<http://www.usdoj.gov/criminal/fraud/idtheft.html>)
- Privacy Rights (<http://www.privacyrights.org.identity.htm>)
- Identity Theft Resource Center (<http://www.idtheftcenter.org.index.shtml>)
- US Federal Trade Commission (<http://www.consumer.gov/idtheft/>)
- Identity Theft Prevention and Survival (<http://www.identitytheft.org/index.htm>)
- 'Scambusters' (<http://www.scambusters.org/index.html>)
- Bank of America (<http://www.bankofamerica.com>)
- National Fraud Information Centre (<http://www.fraud.org>)
- National Institute for Consumer Education (<http://www.nice.emich.edu>)
- International Investigation Services (<http://www.superhighway.is/iis/access.html>)
- 419 Coalition (<http://home.rica.net/alphae/419coal/index.htm>)

Whilst all reasonable care has been taken in the preparation of this information sheet, no liability is assumed by the Commonwealth of Australia for any errors or omissions.

How to report identity theft

Your first point of contact when reporting any identity theft or identity fraud activity, should be your local State or Territory police. However, depending on how your identity has been used, you may need to contact a range of other organisations. This could include Australian, state and local government agencies, finance providers such as banks and credit unions, utility providers and retail stores.

You will also be required to provide written documentation to each of these organisations to support your case and to establish that you are not liable for any debts accumulated in your name.

You will find attached examples of two documents that may assist you in providing this information, and establishing that you were not responsible for fraudulent acts carried out in your good name. These are:

- Statutory Declaration – Identity Theft
- Statement of Fraudulent/Disputed Accounts.

Although these documents are a guide only, they are a useful starting point in reclaiming your good name and limiting the damage done to your identity.

Statutory Declaration — Identity Theft

This 'Statutory Declaration – Identity Theft' should be used as a guide only. The format and text contained in this document are suggestions only. The Commonwealth of Australia accepts no responsibility for any use of this document.

I, _____

_____do solemnly and sincerely declare as follows:

[NAME, address and occupation of person making the declaration]

1. I did not authorize anyone to use my name or personal information to seek money, credit, loans, goods or services.
2. I did not receive any benefit (including money, goods or services) as a result of the events described in this declaration.
3. To the best of my knowledge I believe that my identification documents (eg: credit/debit cards, birth certificate, drivers licence) were stolen/lost on or about _____ (day/month/year).
4. (Description of Fraud) I believe my identity was used fraudulently in the following way(s):

(Attach additional pages as necessary)

5. *(Delete as appropriate)* I have/ have not reported these events to the police.
6. *(Delete as appropriate)* I do/ do not authorise the release of the information contained in this declaration to the police or other law enforcement agencies to assist them in the investigation and prosecution of the person(s) responsible for these fraudulent acts.
7. I have attached the following supporting documentation: *(Delete as appropriate)*
 - Yes/No. Copy of a valid photo identification document (eg: Drivers licence or Passport).
 - Yes/No. Copy of your Birth Certificate (only if you do not have valid photo identification).
 - Yes/No. Proof of residency during the period the fraud occurred (Copy of a rental/lease agreement, copy of a utility bill).
 - Yes/No. Copy of the Police report.
 - Yes/No. A list of fraudulent/disputed accounts opened with your organisation/company without my knowledge or permission using my personal information or identifying documents.

And I make this solemn declaration by virtue of the *Statutory Declarations Act 1959*, and subject to the penalties provided by that Act for the making of false statements in statutory declarations, conscientiously believing the statements contained in this declaration to be true in every particular.

[signature of person making the declaration]

Declared at _____ the _____ day of _____ 20 _____

Before me, _____

[signature of person before whom the declaration is made]

[title of person before whom the declaration is made]

Persons before whom a commonwealth (federal) statutory declaration may be made

The *Statutory Declarations Regulations* provide for a statutory declaration under the Statutory Declarations Act 1959 to be made before the following persons:

Part 1 - Members of Certain Professions

A person who is authorised under a law in force in a State or Territory to practise as a member of any of the following professions:

- Chiropractor
- Dentist
- Legal practitioner
- Medical practitioner
- Nurse
- Patent attorney
- Pharmacist
- Physiotherapist
- Psychologist
- Veterinary surgeon

Part 2 - Other Persons

Any of the following persons:

- Agent of the Australian Postal Corporation who is in charge of an office supplying postal services to the public
- Australian Consular Officer, or Australian Diplomatic Officer, (within the meaning of the *Consular Fees Act 1985*)
- Bailiff
- Bank officer with 5 or more continuous years of service
- Building society officer with 5 or more years of continuous service
- Chief executive officer of a Commonwealth court
- Civil marriage celebrant
- Clerk of a court
- Commissioner for Affidavits
- Commissioner for Declarations
- Credit union officer with 5 or more years of continuous service
- Fellow of the National Tax Accountants' Association
- Finance company officer with 5 or more years of continuous service
- Holder of a statutory office not specified in another item in this Part
- Judge of a court
- Justice of the Peace
- Magistrate

- Master of a court
- Member of the Association of Taxation and Management Accountants
- Member of the Australian Defence Force who is:
 - (a) an officer; or
 - (b) a non-commissioned officer with the meaning of the *Defence Force Discipline Act 1982* with 5 or more years of continuous service; or
 - (c) warrant officer within the meaning of that Act
- Member of the Institute of Chartered Accountants in Australia, the Australian Society of Certified Practising Accountants or the National Institute of Accountants
- Member of the Institute of Corporate managers, Secretaries and Administrators
- Member of the Institution of Engineers, Australia, other than at the grade of student
- Member of:
 - (a) the Parliament of the Commonwealth; or
 - (b) the Parliament of a State; or
 - (c) a Territory legislature; or
 - (d) a local government authority of a State or Territory
- Minister of religion registered under Division 1 of Part IV of the *Marriage Act 1961*
- Notary public
- Permanent employee of:
 - (a) the Commonwealth or of a Commonwealth authority; or
 - (b) a State or Territory or of a State or Territory authority; or
 - (c) a local government authority;
 with 5 or more years of continuous service who is not specified in another item in this Part
- Permanent employee of the Australian Postal Corporation with 5 or more years of continuous service who is employed in an office supplying postal services to the public
- Person before whom a statutory declaration may be made under the law of the State or Territory in which the declaration is made
- Police Officer
- Registrar, or Deputy Registrar, of a court
- Senior Executive Service officer of the Commonwealth, or of a State or Territory, or of a Commonwealth, State or Territory authority
- Sheriff
- Sheriff's officer
- Teacher employed on a full-time basis at a school or tertiary education institution

dealing with identity theft

Statement of fraudulent/disputed accounts

Name Joe Citizen

Address 84 Somewhere Place, Canberra ACT 2601

Telephone: B/H _____ A/H _____

Due to the theft of my identity as described in the attached *Statutory Declaration – Identity Theft*, the following accounts were opened with your organisation in my name without my knowledge, permission or authorisation.

Organisation/Company	Account Number	Type of Credit/Goods or Services Provided	Date Account Opened	Value of Credit/Goods or Services Provided
<i>(Example Only)</i> First Bank of Australia	34821021	Credit Card	01/04/2003	\$10,000.00
<i>(Example Only)</i> First Bank of Australia	42110563	Car Loan	01/03/2003	\$20,000.00

During this time I did / ~~did not~~ have legitimate accounts with your organisation. *(Delete as Appropriate)*

Account Name	Account Number	Type of Account
<i>(Example Only)</i> J & M Citizen	2973482	Credit

I believe that unauthorised transactions ~~did~~ / did not occur with these accounts. *(Delete as Appropriate)*

Attach copies of account statements with disputed transactions highlighted.

- Make as many copies of this document as required.
- Complete a separate form for each organisation you are notifying and attach it to a copy of your completed *Statutory Declaration - Identity Theft*.
- Only include details of accounts relevant to the particular organisation you are notifying.

Statement of fraudulent/disputed accounts

Name _____

Address _____

Telephone: B/H _____ A/H _____

Due to the theft of my identity as described in the attached *Statutory Declaration – Identity Theft*, the following accounts were opened with your organisation in my name without my knowledge, permission or authorisation.

Organisation/Company	Account Number	Type of Credit/Goods or Services Provided	Date Account Opened	Value of Credit/Goods or Services Provided

During this time I did/ did not have legitimate accounts with your organisation. *(Delete as Appropriate)*

Account Name	Account Number	Type of Account

I believe that unauthorised transactions did/ did not occur with these accounts. *(Delete as Appropriate)*

Attach copies of account statements with disputed transactions highlighted.

- Make as many copies of this document as required.
- Complete a separate form for each organisation you are notifying and attach it to a copy of your completed *Statutory Declaration - Identity Theft*.
- Only include details of accounts relevant to the particular organisation you are notifying.

Identity theft quick reference check-list

How vulnerable are you?

Personal documents		yes/no
1	Have you got more credit cards in your wallet than you need? Only carry with you those credit cards you intend to use—leave the rest locked up; only take your ATM card with you if you need to use it.	
2	Did you let your credit card out of your sight when paying a bill? Keep your credit card in sight at all times. Don't give anyone the opportunity to 'skim' your credit card by letting it out of your sight.	
3	Do you leave your personal documents lying around? Keep such documents in a locked safe or filing cabinet. Never leave personal documents out.	
4	Is your home letterbox insecure? An unlocked letterbox is an invitation to a thief to steal personal information from your mail. Make sure you can lock your letterbox, and keep it locked at all times.	
5	Is there anything in your car glove box that could identify you? Remove registration papers, driving licences, bills etc from the glove box—keep such items locked away and only carry them when they are needed.	
6	Do you put sensitive papers in your household garbage bin? Before disposing of personal information, tear up, burn or shred any documents that could assist an identity thief. Home shredders can be used to deal safely with any personal documentation before throwing it away.	
7	Do you give anyone your credit card details over the phone? Be sure these details are being used for a legitimate purpose, and check your credit card statement to make sure you have not been made a victim of identity theft.	
8	Do you buy goods or services on the internet? Make sure the business site contains a full statement on its privacy policy. Also check the site you are accessing is a secure site.	
9	Are you forgetting to check your credit report regularly? Check your credit report regularly to make sure nobody has been misusing your personal information for criminal purposes	

Computer records		yes/no
10	Are you forgetting to change your ISP password regularly? It is a good idea to change your password every month. This is a deterrent to anyone thinking of accessing your personal records through your computer.	
11	Do you keep personal information on your computer hard disk? Save personal information, particularly financial, to a floppy disk. Leaving it on your hard disk makes it easy for a hacker to access it and steal it. Consider encryption software. Don't use automatic log-in features that save your password.	
12	Do you forget to regularly update your virus protection? Out-of-date virus protection is like having no protection at all—install updates regularly. Never open attachments that you are not expecting without running your virus protection. Viruses can be attached to emails as well—do not open mail from unknown sources.	
13	Do you use public access computers? Be wary about using computers in public libraries, at airports and in internet cafés—don't use them to access your private information, as personal details may be retrievable from the computer by identity thieves.	
14	Do you lack a personal firewall protection? A firewall will stop unauthorised access to your computer. Firewall programs are particularly important if you use a high speed internet connection and leave your computer connected 24 hours a day.	

If you have answered 'yes' to any of the above, then you may be a potential victim of identity theft.

If the worst comes to the worst ...

- Report identity theft to the police**
 Identity theft is like any other theft—it must be reported to the police. Provide all documentation necessary to assist the police in investigating the crime.
- Contact the Credit Reporting Agency**
 Report that you are a victim of identity theft. Ask that an alert be placed on your file, and ask that you be contacted by phone if credit providers want to open accounts for you. Accessing your credit file is free—you should not be asked to pay a fee.
- Check your credit file carefully for unauthorised entries**
 Look for accounts that have been opened in your name, or unauthorised changes to your existing accounts.
- Close all accounts**
 Contact all the businesses with whom unauthorised accounts have been opened in your name and ask them to close all fraudulent accounts. Also close all legitimate accounts and open new accounts with new PINs and passwords.
- Keep all documentary evidence of fraud**
 Take notes, keep copies, keep police reports, get confirmation of conversations and actions in writing. Never send originals away in the mail—if documents are required by someone else, send photocopies.
- With police help, take action to clear criminal records**
 Your first point of contact is the police—you may have to undergo police routines of photographing and fingerprinting to establish that you are not the same person as the person who stole your identity and used it fraudulently. You may need to hire a lawyer—Legal Aid or the Law Society in your state or territory may be able to assist.

Whilst all reasonable care has been taken in the preparation of this information sheet, no liability is assumed by the Commonwealth of Australia for any errors or omissions.

References

Australasian Centre for Policing Research, 2003, Australasian Identity Crime Policing Strategy 2003 – 2005, SA.

AUSTRAC 2000, Proof of Identity, Canberra.

National Office for the Information Economy, 2002, The Current State of Play, Available [http://www.noie.gov.au/projects/framework.Progress/ie stats/CSOPApril2002/start.htm](http://www.noie.gov.au/projects/framework.Progress/ie%20stats/CSOPApril2002/start.htm)

Ringin, S. 2001, To investigate ways to counter the production and use of counterfeit documents. Report to the Winston Churchill Memorial Trust of Australia by Shane Ringin – 2000 Churchill Fellow.

Rusch, J. 2002, 'Sweeping Up After Identity Theft' osOpinion, Available: <http://www.osopinion.com/perl.story/18967.html>