

ISBN: 1 921241 98 5

© Commonwealth of Australia 2009

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, 3-5 National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>

Published by the Australian Government
Attorney-General's Department (Job No. 4898).

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

For other business information go to
www.business.gov.au

Additional copies of this booklet are available
from the Attorney-General's Department website
www.ag.gov.au/identitysecurity
or by emailing identity.security@ag.gov.au



Australian Government



Dealing with **identity theft**

Protecting your Identity

Contents

What is identity theft?	4
Why is identity theft such a problem?	5
How does identity theft happen?	6
What can be done with a stolen identity?	7
What if I find someone else's identity document?	7
What can you do to protect your identity?	8
Protect your personal information	8
Protect your financial information	11
Protect information on your computer	12
How do I know if somebody has stolen my identity?	14
What should I do if I am a victim of identity theft?	15
Whom should I contact?	17
Police	17
Lost or stolen citizenship certificate, visa or other immigration document	18
Lost or stolen Medicare card	18
Credit reporting agencies	18
Lost or stolen driver's licence	18
Lost or stolen birth, marriage, death or change of name certificate	19
Lost or stolen passport	20
Lost or stolen foreign documents	20
Other important contacts	20
ATM and credit cards, mobile phone	21
Identity theft—checklist	22

Foreword

The Australian Government is concerned about the incidence of identity crime in Australia and internationally. Identity crime refers to offences in which a perpetrator uses a false identity in order to facilitate the commission of a crime. Identity crime is sometimes referred to as identity fraud, or identity theft.

Being able to prove you are who you say you are is an important part of modern life. You often have to identify yourself to receive services and conduct normal everyday transactions.

This booklet provides information on the risk identity theft poses to each and every member of the Australian community.

It provides practical strategies on how to prevent yourself from becoming a victim of identity theft, and what to do if you do become a victim of this devastating crime. Key areas include:

- protecting your personal information
- protecting your financial information
- protecting personal information on your computer, and
- what to do if you are the victim of identity theft.

By establishing effective identity security routines at home, and in your daily life, you will not only be protecting your personal identity, but also be contributing to the preservation of Australia's national security and economic interests.

I urge you to protect your identity and that of your family and your business. This booklet will guide you through the steps to achieve this and also refer you to other government resources. Keep it on hand as an important reference guide.

The Hon Robert McClelland MP
Attorney-General

What is identity theft?

Identity theft refers to the fraudulent practice of using another person's name or other personal information, usually for financial gain.

Identity theft can occur in many ways—from somebody using your credit card details illegally to make purchases, through to having your entire identity assumed by another person to open bank accounts, take out loans and conduct a business in your name.

Unfortunately, identity theft is a growing part of Australian life. While technological advances such as the internet have improved communications and the ease of doing business, the downside is that fraudsters and other criminals may have more opportunities to obtain details about you, your home and personal life.

The result is that Australians are being exposed to greater risk of identity theft if they do not adequately protect their personal information.

Once an identity thief has enough of your personal information, they may be able to:

- trick your bank or financial institution into giving them access to your money and other financial accounts
- open new accounts in your name, accumulate huge debts and ruin your credit rating and good name or perhaps worst of all
- use your name to commit further crimes, or to plan and even carry out terrorist activity.

Unfortunately, you may not even know you are the victim of identity theft until long after this has happened.

Why is identity theft such a problem?

Identity theft is an ongoing threat and hundreds of thousands of people worldwide become victims every year.

It is essential to Australia's security and economic interests that the identities of persons accessing government services, benefits, official documents and positions of trust can be verified. Protecting the identities and financial welfare of Australian citizens is central to our national security and economic interests.

Identity theft can be devastating to individuals, business, and government. The misuse of false or stolen identities can not only result in the theft of money, but can be used:

- for terrorist acts and other criminal activity
- to breach border protection and citizenship controls and
- to support financial crime, including money laundering, and terrorist financing.

Victims of identity theft bear significant financial and emotional costs and may experience difficulties in regaining control of their identity and restoring their credit rating.

In 2007 the Australian Bureau of Statistics conducted a survey on personal fraud. The findings indicated that around half a million Australians, 3 per cent of the population aged 15 or more, experienced some form of identity fraud in the 12 months preceding the survey.

Public perception of the danger of identity theft is even higher. In 2007 the Office of the Privacy Commissioner commissioned a national survey which found that 9 per cent of respondents, aged 18 or more, claimed to have been victims of identity theft and that 60 per cent were concerned about becoming a victim. Forty-five per cent of respondents believed that identity theft was likely to occur as a result of using the Internet.

How does identity theft happen?

Your identity is a valuable asset—to both you and criminals. Modern life requires us to identify ourselves everyday—you need to prove your identity to open a bank account or get a loan, receive registered mail, interact with a government agency or enter your workplace.

With enough information, identity thieves can pretend to be you, and interact with business and government agencies using your name. If they do this, you can be sure that they won't be doing anything good. How can they do this? There are numerous ways that identity thieves can access your personal information.

- You may lose your purse/wallet/handbag or have it stolen—you probably carry more personal information than you realise.
- Your home may be broken into and personal papers stolen.
- Thieves may steal mail from your unsecured letter box.
- Thieves may retrieve information from your recycling or waste paper bin.
- You may provide your personal details over the phone or internet to what may appear to be a legitimate business.
- As a customer, your details may be stored on a business computer system. This may be illegally accessed by outsiders or, worse still, corrupt employees may deliberately sell your personal information.

You need to protect evidence of your identity as carefully as you protect your most valuable possessions.

What can be done with a stolen identity?

Here are some examples of types of fraud criminals can perpetrate using your name:

- opening new credit card accounts using your name
- opening a bank account in your name and writing fraudulent cheques on the account
- buying a mobile phone and opening a phone account in your name
- buying cars with loans in your name
- writing to your credit card issuers and, pretending to be you, and changing the address on your account. You don't receive statements and don't realise there is a problem until you check your credit report, or
- by accessing publicly available company records fraudsters can change names of company principals and registered addresses and then obtain credit and goods in the company's name.

What if I find someone else's identity document?

If you find someone else's identity document, then it is your responsibility to deliver it to your local police station. For high priority documents (that is, passports, visas, citizenship certificates, birth certificates and driver's licences), the local police will contact the owner to arrange retrieval. If the owner cannot be located, the local police will contact the agency that issued the document.

What can you do to protect your identity?

Although the overall risk of identity theft in Australia remains relatively low, the rate of identity related crime is increasing. It is thus important that each of us take steps now, to protect our name and identity.

The following pages provide a number of quick and easy strategies that you can use in everyday life to reduce the risk of becoming an identity theft victim.

Protect your personal information

- **Lock all personal documents in a safe container when not using them**

By safely and securely storing your personal information and documents, you can prevent them from falling into the wrong hands. Consider storing important documents in a fire/water proof container or safe deposit box.

- **Keep copies of key documents in a secure location**

If possible, make copies of your key proof of identity documents, such as your driver's licence, birth certificate, or passport, and keep these copies in a secure location. Should the originals go missing or be destroyed, the copies could be useful in re-issuing the originals, or to verify claims that you or others may make about your identity based on these documents.

- **Only carry essential personal information**

Unless you really need to, do not carry important documents outside of your home. This minimises the chance of your personal information being lost or stolen.

- **Destroy personal information before putting it in the bin**

You should destroy all old records, files, bills, unsolicited credit card application forms, expired cards—by tearing, cutting up, shredding or burning them before you throw them in the recycling or waste paper bin. Remember to also cut up, or shred, your

old driver's licence, credit cards and storage media, such as CDs, that you have used to store computer files with personal information, prior to disposal. It is not uncommon for thieves to go through your bins in the hope of finding personal records or information.

- **Put a lock on your letterbox**

Ensure you have a secure lockable letterbox or post office box. Remove mail from your home mailbox as soon as possible after it has been delivered. Post mail only at secure, official post boxes. If you move house, notify everyone about your change of address, as mail sent to the wrong address could be used to steal your identity.

- **Do not respond to suspicious mail or e-mail**

Identity thieves may write to you or email you—offering money, or telling you that you have won the lottery—some asking you to share some of your personal details. If you don't know who they are—don't respond.

- **Do not store personal details on mobile phones or wireless devices**

Information stored on mobile or wireless devices is at risk of theft through a Bluetooth connection. You can reduce this risk by de-activating Bluetooth or turning off the 'discoverable' feature.

- **Avoid giving personal or financial information over the phone**

This is especially important with phone calls you didn't make yourself. If you receive an unsolicited phone call from someone wanting to know your personal details—hang up. If you need to provide personal information over the phone, ask for the caller's name and number and contact them yourself.

- **Ask questions**

Do not just accept everything you are told from people who have called offering you ‘the opportunity of a lifetime’. Ask questions if you have concerns. Don’t agree to anything straight away. If you think the offer is legitimate—do some independent research before committing yourself. If the offer sounds too good to be true, it probably is.

- **Activate caller ID on your phone and record the numbers of unusual calls**

By doing this and providing the numbers of suspect phone calls to the appropriate authorities, you can play your part in helping to stop scammers from continuing to defraud. Contact your telecommunications provider for further information on activating caller ID.

- **Contact the Do Not Call Register**

The Do Not Call Register allows individuals to register if they do not want to receive certain unsolicited telemarketing calls. Register via the website www.donotcall.gov.au or by phoning 1300 792 958.

- **Treat any request for copying your personal documents with caution**

Be wary of any businesses that want to take photocopies of your proof of identity documents, such as your driver’s licence. Ask them how the information will be used and stored. However, banks and financial institutions have a legitimate reason for keeping copies as they can assist in investigations, should a fraud occur.

- **Protect your documents when you are travelling**

When you are travelling overseas take extra care of your personal documents. It can be useful to leave a copy of your passport and other key travelling documents with a trusted person at home. Access to a copy can be useful in case of loss or theft of the originals. More information on official documents can be found at www.smarttraveler.gov.au.

Protect your financial information

- **Order a copy of your credit report annually**

By checking your credit report annually you can catch any unauthorised activity. Credit reports can be ordered from one of the three main credit reporting agencies in Australia (listed on p18).

- **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 and limit the damage. By registering for online banking you can check your accounts frequently and do not have to wait for your monthly statement. When you are banking online, ensure that the website commences with 'https' or has the 'closed padlock' symbol displayed.

- **Be wary about giving your personal or financial information to anybody with whom you have not initiated contact**

Anybody contacting you out of the blue and asking for your banking details, is most probably attempting a scam. However, banks and financial institutions may contact you if there is suspected fraudulent activity with your accounts, but they do not ask you to give them details that they already hold.

- **Limit the credit you have in certain accounts**

Use a separate account or credit card with a low credit limit, which is not linked to your other accounts, for transactions over the phone or internet. If the account is breached, any loss will be minimised. Remember, if the loss is not your fault, your financial institution should reimburse you for any money lost.

Protect information on your computer

- **Use passwords and access controls**

By protecting your computer and important documents with passwords and access controls, you make it more difficult for scammers or identity thieves to access information directly from your computer. This is particularly important when operating a wireless connection secure it with a password.
- **Choose strong passwords and change them regularly**

Ensure your passwords contain a mixture of upper and lower case letters, numbers and other characters. Memorise the passwords, and change them regularly. Do not write them down and leave them in an obvious place, such as your wallet.
- **Protect your passwords**

When logging onto a site which requires you to have a logon and password, do not select the option 'would you like the computer to remember this password'.
- **Avoid giving out personal information over the internet**

Only provide the minimum amount of information necessary to those individuals or companies with whom you have initiated contact. Unsolicited e-mails or offers that seem too good to be true or that require you to provide your bank account details or other personal information are almost certainly scams. Don't reply—hit delete.
- **Never click on a link or open an attachment in an e-mail from someone you don't know and trust**

Opening attachments or clicking on links in e-mails can download malicious software into your computer or can redirect you to a fake site. It is much safer to type in the web address yourself, than to rely on a link.
- **Install anti-virus software**

Criminals are constantly developing new viruses and programs to steal or access your personal and financial information. Anti-virus and firewall programs help to block unauthorised access to your computer. Remember to scan your computer's files at least fortnightly and to keep the software updated.

Free software is available from the internet, for more details consult the fact sheet available from Stay Smart Online on <http://www.ssoalertservice.net.au/fact-sheets>

- **Exercise caution when using social networking sites**

Be careful about revealing personal and/or financial information when using social networking sites, internet dating sites or chat rooms. If you use social networking sites, be sure to set your profile to 'private'. It is also better not to share your date of birth. If you receive unusual requests from a friend via a social networking site, verify it via another source before undertaking action such as sending money.

- **Avoid using public computers to access your personal information**

Any personal information you access using a public computer, including passwords, credit card and account numbers, may be retrievable from the computer's hard drive by anyone with the appropriate skills. If you do use a public computer, clear the history and close the web browser before you leave the terminal.

- **Secure computer disposal**

If you are selling or otherwise disposing of your computer, ensure that no personal information remains on your hard drive. Deleting files and emptying the recycle bin or even formatting the hard drive on your computer will not be enough. Deleted files can be undeleted and formatted hard drives can be recovered. To reduce this risk, you should use a 'wiping' or 'erasing' software.

- **Mobile phone disposal**

Similarly, ensure that no personal information remains on your mobile phone before you sell or otherwise dispose of it. The best way is to remove the SIM card. Check with your telephone's manufacturer for instructions on how to prepare your telephone for recycling.

**For more tips check out the following website:
www.staysmartonline.gov.au**

How do I know if somebody has stolen my identity?

Here are some warning signs that indicate that somebody could be using your identity.

- **Missing wallet or purse**

If you have lost your wallet or think it has been stolen it may be returned to you. Even if it seems to be intact, there is a possibility that your personal details have been copied and that your identity is at risk of being stolen.

- **Unfamiliar charges or withdrawals**

Always check your bank and credit card statements and make immediate inquiries if you detect charges and withdrawals you do not recall making. By registering for internet banking you can check your statements online anytime.

- **Unfamiliar Bills**

If you receive bills for goods or services that you did not order, this could indicate that somebody has used your name fraudulently.

- **Missing mail**

If your bills and other mail have gone missing, or you have noticed a reduction in mail, it is possible that mail has have been stolen from your letter box or redirected to a new address without your authorisation. Check with your post office whether anybody has lodged an order to redirect your mail.

- **Calls from Creditors**

If you are being contacted by creditors with whom you did not do business, you need to take immediate action to find out who has been dealing with them. Make it clear to the creditor that you have not engaged in those transactions.

- **New Credit Cards**

If you receive new credit cards that you did not apply for, contact the issuer without delay to have them cancelled, clarify that you did not apply for them, and attempt to establish who did lodge the application.

- **Denial of Credit**

Unexplained refusal of credit requires investigation on your part. You need to get access to your credit report without delay.

What should I do if I am a victim of identity theft?

If you do become a victim of identity theft, there are certain steps you can take to minimise any financial loss and damage done to your name. However, it is important to remember that, even if you do follow all these steps, it may not prevent unauthorised or fraudulent use of your documents.

- **Immediately inform the police**

All incidents of identity theft should be reported to your local police even if only small sums are involved. Ask for a copy of the police report—most banks or other financial institutions will ask you for a copy.

- **Close all unauthorised accounts**

Contact the credit providers and businesses with whom any unauthorised accounts have been opened in your name. Remember this includes phone and other utility providers, department stores and financial institutions. Inform them that you have been a victim of identity theft and ask them to close the fraudulent accounts.

- **Alert your bank or financial institution**

Contact your bank or financial institution immediately and cancel all cards and accounts that may have been breached. Ask for new cards and accounts with new Personal Identification Numbers (PINs).

- **Get a copy of your credit report**

Inform the credit reporting agencies that you are a victim of identity theft (see p 18). Ask that an alert be placed on your file that advises this. This should stop additional fraudulent accounts being opened in your name.

- **Review your credit report carefully**

Ensure you can authenticate all 'inquiries' made into your credit history. Contact all companies and organisations that have made inquiries under your name that you did not authorise.

- **Keep all documentation**

Take notes that include dates, names, contact details and what was said during your contact with those agencies. Follow up all conversations and requests in writing, and send these by certified mail if you need to post them. Keep copies of all forms and correspondence. You can find sample copies of complaint letters in the Australian Securities & Investment Commission's 'How to complain' booklet, available at www.fido.gov.au.

- **Report loss or theft of documents to the relevant government or private sector agencies**

Contact the relevant government and private sector agencies if you have lost specific documents or items, or had them stolen.

- **Contact the Office of the Privacy Commissioner if you feel your privacy has been breached**


If you feel that your privacy has been breached because of identity theft, or an agency or organisation or credit rating agency is being difficult about rectifying matters, then you can contact the Office of the Privacy Commissioner (see p 20). However, it is important that you first try and resolve matters with the agency concerned and only contact the Privacy Commissioner as a last resort.

Whom should I contact?

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


Police

NEW SOUTH WALES POLICE

 131 444


www.police.nsw.gov.au

VICTORIA POLICE

 (03) 9247 6666


www.police.vic.gov.au

QUEENSLAND POLICE

 (07) 3364 6464


www.police.qld.gov.au

WESTERN AUSTRALIA POLICE

 131 444


www.police.wa.gov.au

SOUTH AUSTRALIA POLICE

 131 444


www.sapolice.sa.gov.au

TASMANIA POLICE

 131 444

www.police.tas.gov.au

AUSTRALIAN FEDERAL POLICE (ACT POLICING)

 131 444


www.afp.gov.au

NORTHERN TERRITORY POLICE

 131 444

www.nt.gov.au/pfes

CRIME STOPPERS

 1800 333 000

www.crimestoppers.com.au

Lost or stolen citizenship certificate, visa or other immigration document

DEPARTMENT OF IMMIGRATION & CITIZENSHIP

☎ 131 881

www.immi.gov.au

Lost or stolen Medicare card

MEDICARE AUSTRALIA

Ph: 132 011

www.medicare.gov.au

Credit reporting agencies

Obtain a copy of your credit report and review it carefully to detect any unauthorised activity

VEDA ADVANTAGE

☎ 1300 762 207

www.mycreditfile.com.au

DUN AND BRADSTREET (AUSTRALIA) PTY LTD

☎ 13 23 33

www.dnb.com.au

TASMANIAN COLLECTION SERVICE

Tasmanian residents

☎ (03) 6213 5555

www.tascol.com.au

Lost or stolen driver's licence

Contact the relevant Authority that issued your driver's licence

NEW SOUTH WALES

☎ 132 213

www.rta.nsw.gov.au

VICTORIA

☎ 131 171

www.vicroads.vic.gov.au

QUEENSLAND

☎ 132 380

www.transport.qld.gov.au

WESTERN AUSTRALIA

☎ 131 156

www.transport.wa.gov.au

SOUTH AUSTRALIA

☎ 131 084

www.transport.sa.gov.au

TASMANIA

☎ 1300 851 225

www.transport.tas.gov.au

AUSTRALIAN CAPITAL TERRITORY

☎ 132 281

www.rego.act.gov.au

NORTHERN TERRITORY

☎ 1300 654 628

www.nt.gov.au/transport

Lost or stolen birth, marriage, death or change of name certificate

Contact the relevant Registrar of Births, Deaths and Marriages that issued your certificate

NEW SOUTH WALES

☎ 1300 655 236

www.bdm.nsw.gov.au

VICTORIA

☎ 1300 369 367

www.bdm.vic.gov.au

QUEENSLAND

☎ 1300 366 430

www.justice.qld.gov.au

WESTERN AUSTRALIA

☎ 1300 305 021

www.bdm.dotag.wa.gov.au

SOUTH AUSTRALIA

☎ (08) 8204 9599

www.ocba.sa.gov.au/bdm

TASMANIA

☎ 1300 135 513

www.justice.tas.gov.au

AUSTRALIAN CAPITAL TERRITORY

☎ (02) 6207 0460

www.ors.act.gov.au

NORTHERN TERRITORY

☎ (08) 8999 6119

www.nt.gov.au/justice/bdm

Lost or stolen passport

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE
If your passport is lost or stolen within Australia:

☎ 131 232

www.passports.gov.au

If your passport is lost or stolen whilst you are overseas, report the loss to the nearest Australian diplomatic or consular mission. A list of missions is here:

www.dfat.gov.au/missions

Lost or stolen foreign documents

If you have lost vital documents, such as a passport, which were not issued by an Australian government agency, then contact the relevant diplomatic or consular mission. A list of foreign missions is here:

<http://protocol.dfat.gov.au/Mission/list.rails>

Other important contacts

CENTRELINK

Fraud Tip-off Line

☎ 13 15 24

Report a suspected fraud online:

www.centrelink.gov.au

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Scamwatch

☎ 1300 795 995

www.scamwatch.gov.au

AUSTRALIAN TAXATION OFFICE

☎ 1800 060 062

www.ato.gov.au

AUSTRALIAN SECURITIES & INVESTMENT COMMISSION

www.asic.gov.au

AUSTRALIAN FEDERAL POLICE HIGH TECH CRIME
OPERATIONS

www.afp.gov.au

OFFICE OF THE PRIVACY COMMISSIONER

☎ 1300 363 992

www.privacy.gov.au

ATM and credit cards, mobile phone

Use this space to write in contact details for your providers/issuers

Bank

Credit Card

Mobile Phone

Other contact details

Identity theft—checklist

How vulnerable are you?

PERSONAL SECURITY	Yes/No
Do you carry all of your credit cards, store cards and ATM cards in your wallet at all times?	
Did you let your credit card out of your sight when paying a bill?	
Do you leave your personal documents lying around your home or office unsecured?	
Do you have your mail delivered to an unlocked home letterbox?	
Do you leave any personal papers in your car's glove box?	
Do you put sensitive papers in your household recycling or garbage bin?	
Do you give anyone your credit card details over the phone?	
Do you buy goods or services on the internet?	
Is it more than a year since you have checked your credit report?	

COMPUTER SECURITY	Yes/No
Do you forget to regularly change your Internet Service Provider (ISP)/ email password?	
Do you keep personal information on your computer's hard disk?	
Is your virus protection software out of date?	
Is it more than a fortnight since you have scanned your computer for viruses?	
Do you lack personal firewall protection?	
Do you use a wireless internet connection without protecting it with a password?	
Do you use public access computers?	
Do you post personal information on a social networking site?	

The greater the number of 'yes' responses, the more vulnerable you are to become a victim of identity theft.