Identity Crime

What is identity crime?

Identity crime is a critical threat to the Australian community. This crime type generates significant profits for offenders and causes considerable financial losses to the Australian Government, private industry and individuals.

A set of standard definitions were developed by the Australian Transaction Reports and Analysis Centre's Proof of Identity Steering Committee for use by law enforcement throughout Australia (ACPR 2006:15):

- The term **identity** encompasses the identity of natural persons (living or deceased) and the identity of bodies corporate
- **Identity fabrication** to be used to describe the creation of a fictitious identity
- **Identity manipulation** to be used to describe the alteration of one's own identity
- **Identity theft** to be used to describe the theft or assumption of a pre-existing identity (or significant part thereof), with or without consent and whether, in the case of an individual, the person is living or deceased
- **Identity crime** to be used as a generic term to describe activities/offences in which a perpetrator uses a fabricated identity; a manipulated identity; or a stolen/assumed identity to facilitate the commission of a crime(s).

On this page:

- What is identity crime?
- What does identity crime cost in Australia?
- What is being done about identity crime in Australia?
- What does a criminal do with my personal information?
- How can I protect myself from becoming a victim of identity theft?
- How can I tell if I'm a victim of identity theft?
- If I'm a victim, am I responsible for any fraudulent credit card or bank transactions?
- Certificates for victims of Commonwealth identity crime
- Who can I contact for more information?
- Who can help me?
- Useful links

What does identity crime cost in Australia?

Recent estimates by the Attorney-General's Department indicate that identity crime costs Australia upwards of $1.6 billion each year, with the majority (around $900m) lost by individuals through credit card fraud, identity theft and scams.

More alarmingly, identity crime continues to be a key enabler of serious and organised crime, which in turn costs Australia around $15 billion annually.

Visit the Australian Bureau of Statistics <https://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0/> for more statistics and information on identity crime and fraud in Australia.

What is being done about identity crime in Australia?

The AFP, in collaboration with other government departments and private sector organisations, is involved in a variety of activities to tackle identity theft and identity crime.

The joint AFP and New South Wales Police Identity Security Strike Team (ISST) based in Sydney is supported by the Department of Immigration and Border Protection and New South Wales Roads and Maritime Services.

ISST is dedicated to the investigation of identity related crime, including the compromise of personal information and the production of false or forged documents.

The ISST is focused on investigating serious and complex identity crime matters and form a collaborative network among law enforcement agencies to effectively deal with this crime type.

The ISST works in close cooperation with state police to target the groups responsible for this activity.

What does a criminal do with my personal information?

Once a criminal has the information they need they could:

- apply for a credit card in your name
- open a bank or building society account in your name
- apply for other financial services in your name
- run up debts (e.g. use your credit/debit card details to make purchase) or obtain a loan in your name
- apply for any benefits in your name (e.g. housing benefit, new tax credits, income support, job seeker's allowance, child benefit)
- apply for a driving licence in your name
- register a vehicle in your name
- apply for a job/employment in your name
- apply for a passport in your name
- apply for a mobile phone contract in your name.

How can I protect myself from becoming a victim of identity theft?

You can take some simple steps to reduce the risks of having your personal information stolen or misused:

- secure your mail box with a lock and make sure mail is cleared regularly
- shred or destroy your personal and financial papers before you throw them away, or keep them in a secure place if you wish to retain them
- always cover the keypad at ATMs or on EFTPOS terminals when entering your PIN, and be aware of your surroundings— is anyone trying to observe or watch you, are there any strange or loose fixtures attached to the machine or terminal?
- ensure that the virus and security software on your computers and mobile devices is up-to-date and current
- don't use public computers (for instance, at an internet café), or unsecured wireless 'hotspots', to do your internet banking or payments
- be cautious of who you provide your personal and financial information to—ensure that there is a legitimate reason to supply your details. Don't be reluctant to ask who will have access to your

information and which third parties it may be supplied or sold to. Ask to see a copy of the Privacy Policy of the business before you supply your details

- only use trusted online payment websites for items won at online auctions or purchased online. Never make payments outside of trusted systems—particularly for goods which you have not yet received
- regularly review your bank statements and obtain a copy of your credit history report. Report any unauthorised transactions or entries ASAP
- ask your bank or financial institution for a credit or debit card with an embedded 'micro-chip'—they are more secure than cards with only magnetic stripes
- don’t respond to scam emails or letters promising huge rewards if bank account details are supplied, or in return for the payment of 'release fees' or 'legal fees'
- if responding to an online employment or rental advertisement, be wary of transmitting personal information and copies of documents via email or electronically. If asked to attend an interview, do some prior research to confirm the legitimacy of the company or employment agency
- in relation to social networking sites, always use the most secure settings. Take extreme care if placing personal details such as date of birth, address, phone contacts or educational details on your profile, and don’t accept unsolicited 'friend' requests
- for other useful tips, refer to **protecting your identity resources ‹https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-protection-recovery›** , published by the Department of Home Affairs.

How can I tell if I'm a victim of identity theft?

You may become a victim of identity theft if:

- you have lost or had stolen important documents such as your passport or driving licence
- mail expected from your bank has not arrived or you are receiving no post at all.

You may already be a victim of identity theft if:

- items have appeared on your bank or credit card statements that you don’t recognise
- you applied for a government benefit but are told that you are already claiming
- you receive bills, invoices or receipts addressed to you for goods or services you haven't asked for
- you have been refused a financial service, such as a credit card or a loan, despite having a good credit history
- a mobile phone contract has been set up in your name without your knowledge
- you have received letters from solicitors or debt collectors for debts that aren't yours.

If I'm a victim, am I responsible for any fraudulent credit card or bank transactions?

If you have been a victim of identity crime and your card is still in your possession, you shouldn’t have to pay for anything bought on it without your permission (subject to the terms and conditions of your account).

If your card has been reported lost or stolen, you will usually not have to pay, unless it can be shown that you have acted fraudulently or without reasonable care, for example by keeping your PIN number written down with your card. The same applies to any money lost through fraudulent bank transactions.

Certificates for victims of Commonwealth identity crime

The Attorney-General's Department administers a scheme associated with the provision of certificates where an individual or a business is the victim of Commonwealth identity crime.

If you or your business is a victim of identity crime and you have a Commonwealth Victims' Certificate, you may present the certificate and any other relevant information to a government agency or other organisation. The certificate will help support your claim that you have been a victim of Commonwealth identity crime and will allow you to seek assistance in rectifying problems you have suffered as a consequence of the crime. The certificate doesn't, however, bind an organisation to take action.

Visit the Home Affairs website for more information about **Commonwealth Victims' Certificates ‹https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-crime#content-index-2›** .

Who can I contact for more information?

Information about new methods of identity crime and emerging scams can be found at **SCAMWatch ‹http://www.scamwatch.gov.au/›** — a website run by the Australian Competition and Consumer Commission.

If you would like to report a scam you can complete the SCAMWatch online form form or report it via the **ReportCyber ‹https://www.cyber.gov.au/report›** website.

Reports made to ReportCyber may be referred to police for consideration and possible investigation. If you believe a crime has been committed you should report the scam to **ReportCyber ‹https://www.cyber.gov.au/report›** .

Visit the Home Affairs website for more about **securing your identity ‹https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-protection-recovery›** .

Who can help me?

If you think you have been the victim of identity crime, report the matter to your local police.

Useful links

On our website

- **Online fraud and scams**
- **High tech crime**

On other websites

- **Australian Bureau of Statistics ‹http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0/›**
- **Australian Payments Clearing Association ‹http://www.apca.com.au/getsmart/›**
- **Department of Home Affairs ‹https://www.homeaffairs.gov.au/›**
- **iDcare ‹http://www.idcare.org/›**
- **ReportCyber ‹https://www.cyber.gov.au/report›**
- **SCAMwatch ‹http://www.scamwatch.gov.au/›**

- Stop ID Fraud ‹http://www.stopidfraud.com.au/›