Fellowes
WORK BETTER™

A Guide to Protecting Your Identity

KEEP IT CONFIDENTIAL

with **The World's Toughest Shredders™**

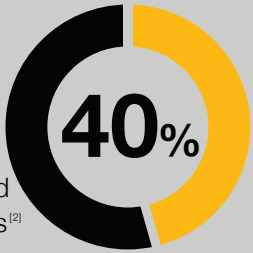
Identity fraud is not just something that happens online – hard copies of sensitive information also provide a high level of risk. Private information such as your date of birth, mother's maiden name and passwords are as valuable as money. This is enough information for a fraudster to open bank accounts, apply for credit cards, loans and much more.

- A growing number of Australians are being impacted by identity crime, which is now one of the most prevalent crime types in Australia[1].
- **1 in 10** Australians reported having their personal information stolen or misused in the previous12 months[1].
- **1 in 5** Australians reported they were a victim at some point in their life[1].
- Identity crime continues to be of great concern to Australians, with around **96%** of respondents to the surveys perceiving misuse of personal information to be a very serious or somewhat serious issue[1].

The total annual estimated economic impact of identity crime in Australia is approximately

$2.4 Billion[2]

IDCrime accounts for of all Police recorded fraud and deception offences[2]



When Fraudsters Strike

Jill, an international student, had been working part-time while studying in Australia. When it came time to lodge her income tax return she wasn't sure of what to do. But instead of phoning the Tax Office or a registered tax agent, she accepted an offer of help from Ram, another international student.

She gave Ram her TFN and other personal details so he could complete her tax return, which she then lodged with the Tax Office and received a tax refund. But once she left Australia, Ram used her TFN to lodge false tax returns and open bank accounts in her name.

Fortunately the Tax Office detected the false returns and Ram was arrested. Meanwhile Jill returned to work in Australia and found she had problems using her TFN as a result of Ram's crimes. It caused her considerable stress constantly having to prove her identity had been misused.

Owner's, Occupiers and Professionals living in the suburbs are often at greater risk

More than two-thirds of Australians are concerned about becoming a victim of identity theft and fraud in the coming year[1]

What do fraudsters look for?

Fraudsters use a variety of ways to gain the information they need to commit ID fraud. Central to all their techniques is the exploitation of the opportunities many of us leave for them.

They just look for easy opportunities to exploit, such as using personal documents that have been thrown away and not shredded or impersonating an official body to trick you into revealing personal information. Therefore much can be done to protect your identity by simply taking basic precautions and reducing the opportunities fraudsters could exploit.

How Identity Theft Happens

BIN RAIDING
Fraudsters pay people to go through the rubbish you throw out, looking for bank and credit card statements, pre-approved credit offers, and tax information.

CARD SKIMMING
This usually occurs when a shop assistant or waiter, for example, gets your information by 'skimming' or copying your credit card information when you make a purchase.

INTERNET SITES
Fraudsters can combine the personal information you provide to unsecured internet sites such as your mother's maiden name with other bits of valuable information they glean about you to obtain credit in your name.

PHISHING
Fraudsters will send an email claiming to be from a bank, Credit Card Company or other organisation, with which you might have a relationship, asking for urgent information. Typically the email will ask you to click on a link to enter your account details on the company's website to protect against fraud or to avoid your account being deactivated. But if you click on the link in the email you will be taken to a website which looks genuine but has in fact been created by fraudsters to trick you into revealing your private information.

THEFT OF WALLET OR PURSE
The average purse or wallet contains bank cards, credit cards and valuable identity documents including driving licenses and membership cards. Victims realise very quickly that their wallet has been stolen but often do not realise the value of the information contained within it until it is too late.

UNSOLICITED CONTACT
Phone calls claiming to be from banks asking you to update your personal information should be regarded with caution. Similarly, fraudsters posing as market researchers may ask for personal information over the phone. Credible organisations will not mind you double checking their authenticity before providing such information.

What is ID fraud?

Identity fraud is when another person uses your personal information to commit fraud. It can be as simple as fraudsters using your credit card to buy things online, to taking out loans in your name, to using your personal information to secure important documents, such as a driving license or passport to commit fraud or more serious crimes.

The Solution?

Shred anything you wouldn't want in the hands of a stranger!

What should you do if you think you've been a victim of ID fraud?

Put a fraud alert on your credit report.

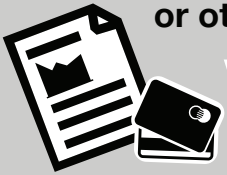
A fraud alert puts a red flag on your credit report and notifies lenders and creditors that they should take extra steps to verify your identity before extending credit.

Get a copy of your credit report. This will show whether fraudsters have tried to open an account in your name.

If you do discover transactions on statements or have loans or other financial products taken out in your name

which you did not make,

contact the provider immediately.



Report all lost or stolen documents,

such as passports, driving licences, plastic cards, cheque books to the relevant organisation.

Contact the Australia Post if you suspect your mail is being stolen or that a mail redirection has been fraudulently set up on your address.**

Top 10 steps to beating ID Fraud

1. Treat your personal information and the documents that carry it as you would treat any valuables.

2. If you are disposing of any documents which contain your personal information on, ensure they are destroyed, such as using a shredder.

3. Regularly update your computer firewall, anti-virus, anti-spyware programmes and delete your web browser and cookie history.

4. Use a variety of **strong passwords** for different online accounts and **never share** them or write them down.

5. Avoid visiting websites which require your personal and financial information in public Wi-Fi areas.

6. If you are asked to supply any personal information by e-mail, mail, the phone or by any other means always check them out and if in doubt do not disclose.

7. **Always report any lost or stolen documents** such as passport's, driving licenses, bank cards, cheque books etc.

8. Always check your statements for any transactions you did not make.

9. Check handbags, shared letterboxes, window sills and hallway tables for personal information that may have been forgotten about.

10. If you move house inform all relevant organisations and redirect mail to the new address.

Fellowes Shredders and PrivaScreen™

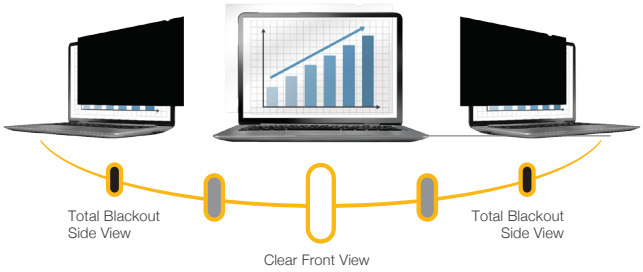
Keep it Confidential

Shredders can be used in all work and home environments to shred confidential documents to protect your identity. While there are different types of security available, a cross-cut shredder gives better protection against ID fraud as confetti-cut pieces become extremely difficult to reassemble.

Use our Shredder Selector Tool to find a shredder that is right for you

Protect yourself on mobile, tablet and laptop

With mobile devices being used more in public, privacy protection has become an increasingly important issue. “Shoulder surfing” is a growing form of identity theft in which private on-screen information is either viewed or photographed over the shoulders of anyone using a mobile device. Whether you use a smart- phone, laptop or tablet, you can protect your privacy in public with PrivaScreen™ Filters.



PrivaScreen™ Filters blackout the screen image when viewed from 30° side angles to prevent prying eyes from reading your screen. Yet on-screen data is clearly visible from a straight-on view, allowing you to work worry-free, even on the go.

Use the Fellowes® Perfect Fit Selector Tool to automatically detect your screen size and suggest which PrivaScreen™ filter is right for you.

Useful contacts

ATTORNEY-GENERAL'S DEPARTMENT:
www.ag.gov.au

AUSTRALIAN FEDERAL POLICE (AFP):
www.afp.gov.au

AUSTRALIA POST:
www.auspost.com.au

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION (ASIC):
www.asic.gov.au

CRIME STOPPERS AUSTRALIA:
Crime Stoppers allows people to phone in anonymously with information about criminals or crimes which is then passed on to the police.

Tel: 1800 333 000
www.crimestoppers.com.au

ID Care:
www.idcare.org/contact/

OAISC:
www.oaic.gov.au

www.fellowes.com/au

[1] Identity Crime and Misuse in Australia Survey, conducted by the Australian Institute of Criminology for the Attorney-General, May 2013

[2] Identity Crime and Misuse in Australia 2013-14 conducted by the Australian Institute of Criminology for the Attorney-General