

PROTECTING

YOUR

IDENTITY



A

PRACTICAL

GUIDE

# CONTENTS

<b>Introduction</b>	<b>1</b>
<b>What Are Identity Theft and Identity Fraud?</b>	<b>2</b>
<b>How Can Your Identity Be Stolen?</b>	<b>3</b>
<b>What Can Be Done With Your Stolen Identity?</b>	<b>5</b>
<b>Preventing Identity Fraud</b>	<b>6</b>
<b>Simple Ways For Businesses To Protect Themselves</b>	<b>9</b>
<b>How To Spot Identity Fraud</b>	<b>11</b>
<b>What To Do If You Become A Victim</b>	<b>12</b>
<b>It Could Happen To You</b>	<b>13</b>
<b>Useful Contacts</b>	<b>14</b>

## INTRODUCTION

When we think of crime we usually think of a physical action or violation against a person or a thing such as burglary, mugging or pick pocketing. However, in the twenty-first century, crime is taking a far more sophisticated form. One of the fastest growing crimes is identity theft and it can be perpetrated without the criminals even breaking into your home. In a recent survey commissioned by Fellowes and conducted by Galaxy Research, 87% of Australians claimed to be concerned about the risk of Identity Fraud, yet 75% of them put themselves at risk by not disposing of documents with due care.

In 2001, the Attorney General's Office estimated that the cost of identity related fraud in Australia exceeded \$4billion per annum. This practical guide explains what identity fraud is, how your identity can be stolen (identity theft) and the different types of identity fraud that can be committed using your name.

It also offers you some simple steps to protect yourself and your business from becoming a victim, and a guide of what to do if your personal or company information is used fraudulently.

# WHAT IS IDENTITY THEFT AND IDENTITY FRAUD?

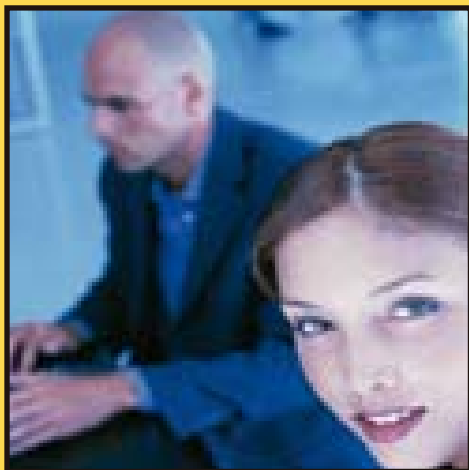
**Identity theft** occurs when an individual's or company's personal or confidential information is obtained by another person in order to assume their identity. Identity theft is the first step to perpetrating a criminal activity whereby criminals may use personal information to obtain credit, goods or other services fraudulently. This is known as identity fraud.

**Identity fraud** can involve setting up a bank account in someone else's name, applying for a credit card or stealing personal details in order to fraudulently obtain goods, services, or other financial advantage. It can even extend to securing a passport in their name.

**Corporate identity** theft may include stealing the identity of a company and fraudulently trading under that name without the knowledge of the legitimate company.

Criminals use a mixture of tactics to acquire the information needed to steal another's identity. These range from the very crude, such as taking personal information from a stolen purse or wallet, going through rubbish, to phishing or stealing somebody's identity online. (See **"How Can Your Identity be Stolen?"** for more information).

Worryingly for the victims of identity theft, they often do not realise their identity has been stolen until it is too late and they start receiving demands for loan repayments or bills for goods they have not purchased. In worst case scenarios innocent people have even been arrested for a crime they did not commit. Luckily most victims of identity fraud will not suffer financially. However it can take a considerable amount of time and effort to put right the damage caused (See **"How to Detect ID Fraud"** and **"What To Do If You Become a Victim"**).



# HOW CAN YOUR IDENTITY BE STOLEN?

In recent years, there has been an explosion of ways to collect, store, share - even steal - personal information about you. Your personal information has become big business and can be invaluable to an identity fraudster. Your identity can be stolen in any of the following ways:



## 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. Everyday information that you may not think is important such as old gas, electricity and telephone bills, insurance documents, bank statements and even personal letters and envelopes they were sent in, carry valuable personal information that can be gathered together to steal an identity.

In the UK a bin raiding survey commissioned by Fellowes for National Identity Fraud Prevention Week showed that an alarming 77% of household waste contained at least one or more items which could assist fraudsters in stealing an identity. Research conducted in Australia in May 2007 confirms that 75% of Australians throw their identity out in exactly the same way. With over 8 million households in Australia, that would suggest that over 6 million households are under threat from identity fraud.



## IMPERSONATION OF THE DECEASED

Ruthless criminals have been known to use the identities of deceased people to carry out fraudulent activity. Fraudsters will note the age, date of birth and address of deceased people from announcements relating to the death or the funeral. 'Day of the Jackal' frauds, where the deceased was aged 18 or under, are estimated to represent up to approximately 18% of the total, based on some research from 2004.

## INTERNET

### SITES

Anybody that uses the Internet will regularly be asked to share personal information to gain access to websites and buy goods. 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.

### MAIL

### FORWARDING

By completing change-of-address forms to redirect your mail, fraudsters can receive a wealth of information about you delivered direct to their doorstep.

### PHISHING

This term describes identity theft via email. 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 personal 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. The fraudsters then use the information provided to set about obtaining money from your accounts.



## 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. They often then sell the information to professional criminal gangs. Like phishing, skimming can be used on its own to collect enough information to use your card fraudulently without stealing your entire identity.

### THEFT OF WALLET

### OR PURSE

The average purse or wallet contains bank cards, credit cards and valuable identity documents including driving licences and membership cards. Victims generally 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. Calling the switchboard of the company in question and asking to be put through to the person who called you will help ensure you are not playing into the hands of fraudsters.

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 CAN BE DONE WITH YOUR STOLEN IDENTITY?

A fraudster may use your personal information to get a car loan, acquire a phone/ mobile phone service, utility service, or open a bank account in your name. Such situations can be seriously damaging to your credit history, since you may not realise anything is wrong until you notice unfamiliar charges on your monthly bills or statements or - worse still - you receive demands for payment from a credit card or loan company.

## TYPES OF FRAUD THAT CRIMINALS CAN PERPETRATE USING YOUR NAME INCLUDE:

- ❓ Opening new credit card accounts using your name. When they use the credit cards and don't pay the bills, the non-payment will appear on your credit report.
- ❓ Opening a phone or mobile phone account in your name.
- ❓ Opening a bank account in your name and writing fraudulent cheques on the account.
- ❓ Counterfeiting cheques or debit cards, and draining your bank account.
- ❓ Buying cars with loans in your name.
- ❓ Writing to your credit card issuer and, pretending to be you, changing the address on the account. Statements get sent to the new address, so you don't realise there's a problem until you check your credit report.
- ❓ 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.

# PREVENTING IDENTITY FRAUD

In May 2007, an opinion poll by Galaxy Research, carried out on behalf of Fellowes, showed that 87% of the Australian public were concerned about becoming a victim of identity theft. Additionally, identity theft was of greater concern than other crimes like burglary, mugging and pick-pocketing.

UK research from credit reference agencies reveal that on average it takes 467 days to discover that you are a victim of identity fraud. By managing your personal information carefully, you can substantially reduce the likelihood of becoming a victim of identity fraud. The following tips show you how:

## AVOID AUTO COMPLETE

Software that offers to remember your personal details to save you time when you next fill out a form online should be avoided. While the software itself is not fraudulent, it can make it easier for thieves to access personal information about you if they successfully access your PC.

## BE VIGILANT

Beware of anybody who contacts you (eg. by phone, E-mail, letter, fax, face to face) unexpectedly and asks for personal information or account details, even if they claim to be from your bank, the police or another official organisation like your local council. Ask for their name and a contact number and then check with the organisation in question before responding back.

## CHECK THE URL

When you are online check the web address of the site you are visiting is spelt correctly, as it is possible to be redirected to a similarly named site which is actually fraudulent. Better still, add the website to your favourites folder so that there can be no mistake you are going to the correct home page each time you log on.

## CHECK YOUR CREDIT

## REPORT AT CREDIT

## REFERENCE AGENCIES

It is a good idea to check your credit report regularly to ensure no accounts or credit have been illegally set up in your name. Regular monitoring of your credit report will alert you if someone has been using your identity to obtain credit, ensuring you can not only rectify your credit report as soon as possible, but also stop the fraudster in their tracks. You can obtain a copy of your credit report from one of Australia's two credit reference agencies (See Useful Contacts). The credit reference agencies also offer subscription monitoring services, which will alert you to any changes to your credit report via email or SMS.

## GUARD YOUR CARDS

Minimise the information and the number of cards you carry in your wallet. If you lose a card, contact the fraud division of the relevant credit card company. If you apply for a new credit card and it doesn't arrive in a reasonable time, contact the issuer. Watch cashiers when you give them your card for a credit card purchase and make sure you can see your credit at all times. When you receive a new card, sign it in permanent ink and activate it immediately.

## SHRED ALL DOCUMENTS

Shredding documents is the best way to ensure that criminals cannot build up a profile based on the information you discard in your rubbish. Invest in a powerful shredder and make it standard practice, whether at home or at work, to shred all documents containing personal or financial information before binning or recycling them. Confetti cut shredders provide greater security by cutting paper into small confetti-like particles and also reduce bulk waste. Companies such as Fellowes offer affordable shredders for home and office use. (See Useful Contacts).

## PASSWORDS AND PINS

According to credit reference agencies, personal information such as your date of birth, address and mother's maiden name is enough information for a fraudster to open bank accounts, apply for credit cards, loans and much more. Memorise your passwords and personal identification numbers (PINs) instead of carrying them with you and NEVER share them with anyone else. Avoid using easily available information like your mother's maiden name, your birth date, your phone number, or a series of consecutive numbers and don't use the same PIN for all your cards and accounts.

## PAY ATTENTION TO BILLING CYCLES

Contact creditors immediately if your bills arrive late. A missing bill could mean a fraudster has taken over your credit card account and changed your billing address.

## PERSONAL INFORMATION

Whether on the phone, by mail, or on the Internet, never give anyone your credit card number or other personal information for a purpose you don't understand. Ask to use other types of identifiers when possible.

## PROTECT YOUR POST

Deposit outgoing post in post office collection boxes or at your local post office rather than leaving it in office out trays or similar. If you plan to go away, contact Australia Post about its Mail Holding Service, which helps you avoid that tell-tale pile of unopened mail at your address. The Service will hold your mail and deliver it on your return. (See "Useful Contacts").

## STAY SAFE ONLINE

If you use the Internet, make sure you have the latest security patches and up-to-date anti-virus software installed.

## UPDATE CONTACT DETAILS

A large proportion of identity thefts are perpetrated at previous addresses. If you move house or change phone numbers tell all relevant organisations about the change as soon as possible. Using a mail forwarding service for at least six months is a good way to make sure all post is redirected to your new home and reduces the risk of your personal information getting into the wrong hands.

## USEFUL NUMBERS

Keep a record of the numbers you need to ring if your credit or debit cards are stolen. You have to cancel your cards as soon as possible after they have been stolen to make sure they cannot be misused.



# IT COULD HAPPEN TO YOUR BUSINESS

## Stuart Holden

Stuart, aged 34, had a staggering \$55,000 stolen through fraudulent means from his business and personal bank accounts two years ago.

Stuart runs his own coaching and training company for businesses. He had his wallet stolen whilst attending a training course. He left his jacket on the back of his chair throughout the day and when he got up to leave he noticed his jacket felt lighter- and his wallet had been stolen.

Immediately, he called all his banks to put a stop on his cards, but due to the fact that he was told he did not answer all the security questions correctly, the banks were unable to take any action.

Once he returned home, his wife informed Stuart that someone from the council had called earlier that day, claiming they had a returned cheque from a council tax refund, and were calling to check Stuart's address. She gave the caller their address and corrected him when he got Stuart's mother's maiden name wrong.

Stuart's bank had also called that day. Unable to get in contact with him, they said they would call back later, and reassured his wife that everything was fine.

What in fact had happened was that the criminals had used the personal information from Stuart's credit card, driving licence and conversation with his wife, to fake his identification and fraudulently take \$10,000 from his business card (over the counter from the bank), \$800 from his bank account, \$35,000 from his Visa card, spent \$6,500 to buy a video camera and \$3,000 in a clothing shop.

The incident was seriously stressful for both Stuart and his wife and affected their business and personal accounts. For Stuart, this was a major distraction to his coaching and training business, due to the time spent trying to solve the crime. In total, he experienced four months of "hell", trying to get his identity back and sort out the crime. In addition, Stuart had to go away for

a business trip the day after the incident, and so had to borrow money to fund it. In the end all the money was eventually recovered.

### Key piece of advice from Stuart:

*"I would advise everyone to never use their mother's real maiden name as a security answer, as it is just too difficult to keep it a secret. Use something funny or even stupid, call her Posh Spice or Domestos if you have to. Also, I've learnt to leave my driving licence at home, and to stop carrying all my credit and debits cards with me – you should keep a couple of them at home, just so that you are covered financially if the others are lost. Additionally, you have to be careful with your post and any other documents that contain personal information, try and get in the habit of shredding, it's essential!"*



# SIMPLE STEPS FOR BUSINESSES TO PROTECT THEMSELVES

Of course, it is not just individuals that can fall foul of identity thieves. Businesses also can be targeted by ruthless criminals. Criminals can then trade off the back of the real company's good name to obtain goods and services on credit from suppliers. This is not the only area of risk. Fraudsters can obtain signatures from public records and attempt to attack company bank accounts by purporting to be the signatory on the account.

Companies can put measures in place to make it harder for criminals to use their organisation for criminal activity. Many of the rules that apply to individuals can be adapted to protect companies. Other steps for businesses to consider include:

## CHECK IDENTITY

Always check the identity of your customers, both businesses and consumers. Credit reference agencies offer a wide range of solutions to authenticate and verify the identity of customers to ensure that they exist and are who they say they are.



## COMPANY DETAILS

**1. Check your 'REGISTERED DETAILS' (Directors, Company Secretary and Company Address) at the Australian Securities and Investments Commission (ASIC).** Make sure these are correct and that they have not been fraudulently changed.

**2. Whether you're in the financial services or the corporate sector, keep up to date with ASIC News, ASIC's free monthly e-newsletter, where you'll find out the latest news on:**

? New and amended documents, including consultation papers that you may want to comment on.

? The latest relief you may want to take advantage of.

? Enforcement activities including arrests, chargings, trials and court outcomes.

? People who you won't want to do business with because ASIC has banned them as company directors or from offering financial services.

? Warnings and financial tips about financial services and products.

**3. Do not rely on ASIC records alone if determining whether to lend goods or service on credit.** ASIC is a public record and not a crime prevention service or credit reference agency. Always satisfy yourself that your customer is legitimate through additional means.

## COMPANY BANK ACCOUNTS

Do not allow details of the main company account to be in the public domain where fraudsters may obtain sufficient detail to facilitate an attack on the account through impersonating the signatories.

## DOCUMENT PROCEDURES

Having a well formulated document disposal policy in place, and adhering to it, is the first crucial step in protecting your business and employees from identity fraud.

## STORE SENSITIVE DOCUMENTS

Lock away sensitive documents in a safe place and limit access to these documents to the staff who really need them. Fellowes has produced a Record Management handbook detailing how companies can store sensitive information safely, which offers useful tips and hints, including legal requirements relating to document retention. (See “**Useful Contacts**”).

## LIMIT ACCESS

Make sure that only key members of staff have access to highly sensitive documents, to ensure that information is not falling into the wrong hands.



## SHRED ALL DOCUMENTS

Businesses have a duty of care to protect their customers’ and employees’ information and a legal obligation under the Privacy Act. Shredding information is the best way to dispose of documents securely and to ensure that criminals cannot gain access to sensitive company details fraudulently. Confetti cut shredders provide greater security by cutting paper into small confetti-like particles and also reduce bulk waste. Companies such as Fellowes offer powerful office shredders which can destroy large quantities of paper as well as CDs. (See “**Useful Contacts**”).

## INFORM STAFF

Informing staff about the risks of corporate identity fraud will ensure that they remain vigilant. Ensure your document disposal policy is communicated to all employees. Caution them about the risk of giving out company information online or over the phone without first checking to whom they are giving the information.

## REDUCE THE RISK OF ELECTRONIC HIJACKING

Businesses must be responsible for ensuring that firewall and anti virus software is kept up-to-date. This way staff can securely open legitimate email attachments for viewing.

## EMPLOYEE VIGILANCE

Most employers store personal data relating to their staff. As an employee:

- ❓ **Double check that your records are kept in a secure location.**
- ❓ **Find out who has access to your details at work – they should only be accessed by other employees for legitimate reasons.**

# HOW TO SPOT IDENTITY FRAUD

The best way to spot identity fraud early is to stay vigilant. Monitor your accounts and credit agreements closely as nobody knows your financial habits, or is better equipped to spot fraudulent activity, than you. The following are useful tips to help you spot fraud as soon as it happens:



## MONITOR BILLING CYCLES

A missing bill or bank statement could mean someone has taken over your credit card account and changed your billing address or intercepted your mail. Keep a note of the date you expect bank statements, new cards and utility bills to arrive and contact the relevant parties if they are late.

## CHECK YOUR STATEMENTS

Review bank and credit card statements and keep an eye out for unusual transactions you do not immediately recognise. Do not be afraid to follow up with your bank or credit card company to see if they can provide more information about the transaction if you think it looks suspicious.



## MONITOR YOUR CREDIT REPORT

Unless you check and monitor your credit report frequently with a company credit reference agency to ensure they are up to date and accurate, there is often no way to tell if identity thieves have used your personal information to open credit accounts or other services in your name.

# WHAT TO DO IF YOU BECOME A VICTIM

If you suspect that someone has used your name, or other personal information to get credit or a loan, the following steps can help.

## CONTACT YOUR BANK AND CREDIT CARD COMPANIES

Contact your bank/building society and credit card provider to cancel any cards. Even if not all your accounts have been affected it is worth flagging the issue to other lenders, banks etc so they can monitor your accounts more closely and ensure that the thieves do not access them.

## CONTACT A CREDIT REFERENCE AGENCY

Contact an accredited Credit Reference Agency such as Dun & Bradstreet. Follow their suggested steps to resolve the situation and prevent it happening again. (See **“Useful Contacts”**).

## FREEZE FRAUDULENT ACCOUNTS

Contact the appropriate creditors, banks, phone companies, and utility companies and have them freeze the accounts. You may be liable for some of the fraudulent charges, different issuers have different policies. Most creditors promptly issue replacement cards with new account numbers.

## CALL THE POLICE

Report the crime to the police department that has jurisdiction in your case and request a crime reference number. Though the authorities are often unable to help, a police report and crime number may be necessary to help convince creditors that someone else has opened an account in your name.

## KEEP A RECORD

Because recovering from identity theft can sometimes be a long and complicated process, it's important to keep a record of all communications. Send all letters by registered mail and keep copies. If you think your case might lead to a lawsuit, keep track of how much time you spend dealing with the problem.

## IF YOU HAVE INFORMATION ABOUT A CRIME, CONTACT CRIMESTOPPERS

Crimestoppers has been operating in Australia since 1987. The hotline **1800 333 000** phone number allows people to phone in anonymously with information about criminals or crimes which are then passed on to the police.

# IT COULD HAPPEN TO YOU

## Samantha Green

Samantha and her husband were both victims of identity fraud in 2005. Samantha, 36 years old, became aware of the fact that her identity had been stolen when she tried to withdraw money from her bank account – they refused claiming she was over her credit limit.

After checking her statements, Samantha noticed a number of fraudulent transactions made from her bank account on various Internet shopping sites. Samantha contacted these sites but they were unable to provide her with any information regarding these transactions because of the Privacy Act. Samantha reported the fraudulent transactions to her bank, who reassured her that she need not worry as they would be dealing with it.

Later that month, Samantha's husband received an urgent message from his credit card company, who informed him someone had been using his card in the United States, but that they had put a stop on it. This was not the end though, as Samantha and her husband were told later that month that their business card had a total of \$8,000 worth of fraudulent transactions made on it - all over the Internet.

In total, nearly \$10,000 had been taken from the Greens. In terms of the impact of their lives, it was an immensely stressful period, and trying to reclaim their identity proved equally taxing. This also meant that Samantha was unable to buy her currency online before going on holiday and all her standing orders had been cancelled, which meant she was being chased for unpaid bills. Both Samantha and her husband had to use cash to pay for everything.

### Key piece of advice from Samantha:

*"Make sure you take extra care when you are shopping online or doing Internet banking, as you should never save any of your details on the sites. I have also begun to shred anything with personal details. I've learnt my lesson to be more vigilant when it comes to my identity."*

## Jonathan Evans

Jonathan Evans, 40, had \$22,000 taken out of his account by criminals. Jonathan suspects that the criminals got hold of his details from a number of statements he threw away the week prior to the identity fraud. Using Jonathan's bank account details, the fraudsters called his bank to change his mailing address. They then requested a new card and PIN to be sent to the new address. The criminals transferred \$22,000 out of his bank account. Luckily, Jonathan spotted this transfer two days later, and reported it to his bank. The bank investigated the claim, and returned the money after two weeks.

Jonathan now has to answer extra security questions in order to get information on all his accounts.

However, the impact of having his identity stolen meant that he was unable to do any online shopping or banking for a month. Just two months ago, the same bank was sent a fraudulent letter asking for Jonathan's address to be changed. It seemed the criminals were not stopping there, as another bank informed Jonathan the following month that someone had attempted to open a new account in his name online. The only reason why this was detected was because an unknown address has been entered.

Jonathan is now very careful of disposing of his letters, making sure he shreds anything with his name and address or personal details, and also makes sure all his accounts are monitored.

### Key piece of advice from Jonathan:

*"Always be aware of what transactions are going through your account, even if that means saving every single receipt you have. Straight after the incident I bought a shredder so that I could get rid of my letters safely. After having my identity targeted three times I became very cautious, but now because I shred everything I can throw away my mail with peace of mind. Another thing I have found very useful is to check my credit rating on a regular basis. This way you are made aware of any other addresses or accounts that are linked to you."*

# USEFUL CONTACTS

## **Attorney-General's department**

[www.ag.gov.au](http://www.ag.gov.au)

### **and accompanying useful links:**

<http://www.crimeprevention.gov.au>

[http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention\\_Identitysecurity](http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity)

## **Australian Federal Police (AFP)**

[www.afp.gov.au](http://www.afp.gov.au)

## **Australia Post**

[www.auspost.com.au](http://www.auspost.com.au)

## **Australian Securities and Investments Commission (ASIC)**

[www.asic.gov.au](http://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](http://www.crimestoppers.com.au)

## **Fellowes Australia**

Tel: 1800 331 177

[www.fellowes.com.au](http://www.fellowes.com.au)



[www.fellowes.com.au](http://www.fellowes.com.au)

© Fellowes Inc Item Code 360612