

FRAUD

prevention



protecting
your personal
finances

■ It Pays to be Alert	2
<hr/>	
■ Traditional Types of Fraud	3-4
<hr/>	
■ Hi-Tech Fraud	5-6
<hr/>	
■ Identity Theft	7
<hr/>	
■ Who To Contact	8
<hr/>	

About the Authors

Cameron Cooper is a respected business journalist and corporate writer with 20 years, experience in the industry. He is a regular contributor to *The Australian* and business titles such as *Connexus*, *Vive*, *Management Today* and *My Business*.

Leanne Vale is Fraud Prevention Manager within the Credit Union Services Corporation Australia Industry Association. As a former police officer, now working in the frontline of fighting fraud, she brings considerable experience and expertise to this publication.

It Pays To Be Alert

Financial fraud is big business and takes many forms – from mail and credit card abuses to identity theft and online deception. The statistics are alarming. Frauds committed using stolen personal details or a false identity are estimated to cost Australia \$4 billion a year and account for more than a quarter of all white-collar crime. And Australian credit card companies lose about \$100

million a year to fraud, according to a survey by market analyst Datamonitor. Many of us are vulnerable to fraud. The best way to prevent attacks is to be alert and arm yourself with knowledge. Common financial tools enhance our daily lives, but it's crucial to keep them in the right hands. In this booklet, we discuss various forms of fraud and offer advice on safeguards.

Fightback Against Fraudsters

Things to do

- Keep tax records and other financial documents in a secure place and delete your tax file number from any documents before throwing them away.
- Ensure documents disclosing your credit card number are shredded or torn up. This includes financial statements, pre-approved credit applications and store receipts.
- Sign credit cards immediately upon receiving them from your financial institution.
- Use a locked mailbox to send and receive all mail. If you receive a lot of big mail, get a larger mailbox with a wide slot or consider a post office box. Locked bags are another option for small businesses that receive cheques by mail.
- Monitor bank account statements to ensure they don't include any incorrect transactions. For small business owners, it's good practice to monitor cheque accounts and reconcile payments.
- Check your credit statements regularly. Most customers don't check them often enough. When statements are disputed with financial institutions, early detection of any error is important.
- Photocopy records of your accounts and identification documents. If you become a victim of identity fraud, it will help prove your case to financial institutions. You can also register with credit check providers who will monitor and report on any attempts to obtain credit using your identity.
- Avoid accessing your account information at internet cafes, offices or on shared computers. Public computers can contain viruses that capture your personal banking details.
- Install appropriate security software on your computer, including personal firewalls and up-to-date virus and anti-spyware protection.
- Generally ignore spam emails, chain letters and people claiming to be representatives of government departments or financial institutions. Be suspicious of any correspondence that advises you to forward sums of money or suggests you have won a prize. If it sounds too good to be true, it almost certainly is. It's good practice to delete any emails and attachments from sources you don't recognise.

Things not to do

- Don't carry identification documents such as your birth certificate or passport unless you really need them.
- Don't dispose of receipts and other personal information casually because identity thieves go through rubbish for information.
- Don't use the same password for financial accounts that you use for other services such as video cards or internet connections.
- Don't forget to change your passwords regularly.
- Don't provide your personal or account information over the telephone or internet unless you are certain of the enquiring source.
- Don't give or send your name, bank account details, and copies of your passport, birth certificate or any other personal details to anyone other than legitimate institutions.

Con artists have been laying traps and abusing people's trust from time immemorial. Be on the lookout for the following common tricks.

Postal theft of ID and financial details

Postal mail is a potential goldmine for thieves, who can easily steal new, unsigned credit cards, bank statements and other personal identifying documents from your home letterbox. Buy a lock to protect yourself, and ensure your mailbox is large enough to accept big envelopes (they often contain the most sensitive financial information). Be aware that some crooks will also go through garbage bins in search of personal information, so it is advisable to shred paperwork that lists financial details (such as receipts) before you put them in the rubbish. If your regular mail seems to have stopped arriving, contact the post office – brazen thieves have been known to redirect people's personal mail.

Credit and debit cards

Some disreputable store operators have recently been caught using mini-scanners to swipe credit card details, which are then used to milk money out of accounts. Try to keep your credit or debit card in sight during a transaction. When you receive new cards, sign them immediately and destroy old cards that have expired. Report any lost or stolen cards. Keep up to date with your finances check all financial statements and report unauthorised transactions. With credit cards, writing down your Personal Identification Number, or PIN, is asking for trouble. Memorise it instead. If you must write the number down, do not keep it with your card. And remember, financial institutions will NOT call asking for your PIN or passwords, so do not reveal such information over the phone or through emails.



Traditional Types of Fraud

Cheques

Cheques have been around for a long time, so thieves have worked out many ways to target them. Keep your chequebook in a secure location, and do not pre-sign cheques – that’s an open invitation for thieves to take as much as they like from your account. When posting cheques in the mail, cross them as “Not Negotiable”. Use an ink pen, not pencil, to write your cheques to reduce the chance of them being altered. Ensure you are mailing cheques to a secure postal address, which can reduce the risk of theft and alteration. Reconcile your cheque accounts regularly and report any anomalies to your financial institution without delay.

Telemarketing and phone scams

Some unscrupulous people try to scam money from consumers by calling them and requesting financial details. They pose as legitimate companies or even government agencies. Do not reveal any financial details over the phone, particularly if the caller promises you money in return for the information.

Chain letters

The advent of the internet has seen chain letters become almost an old-fashioned scamming method. However, if you receive mail from any source asking you for money and warning there will be bad luck in store if you do not follow the instructions, ignore it.



Fraud has become significantly more sophisticated in the era of the internet and technological advances such as automatic teller machines (ATMs) and electronic funds transfer at point of sale (EFTPOS). Fraudsters are always on the lookout for new, hi-tech methods of obtaining personal information. Be on guard and, if necessary, seek advice from reputable IT consultants or companies.

ATM use

Recent incidents of “skimming” entail thieves attaching discreet devices to ATMs and using them to record the personal information or passwords of those using the machine on tape or chips. If you suspect someone has tampered with an ATM, don’t use it, and report the matter to the financial institution. When using an ATM, ensure no one can see you entering your PIN, and put your money away quickly before you leave the machine.

EFTPOS

Electronic withdrawals or payments at stores come with some risks. As mentioned previously, always keep your credit or debit card in sight during a transaction to prevent unauthorised scanning of your card. Beware of “shoulder surfing” where people stand close to you and can easily observe you entering a PIN. Destroy EFTPOS receipts if they are not required for tax purposes.

Online banking and purchasing

Using the internet for banking or to buy goods online has made our lives easier but exposed us to significant security risks. One of the first lines of defence on your home PC is to install security software. The software company should alert you to update “patches” to ensure you are protected against new viruses as they emerge. With internet banking, try to avoid transactions at work or in internet cafes, where others might see passwords or log-on details accidentally stored. Do not respond if you are prompted to save your log-on, and change your password regularly to avoid the risk of it being compromised.

When purchasing goods online, you might be offered internet “wallet” services, a single sign-in offering that allows consumers to use the same user name and password at any participating website. They overcome the hassle of managing different user names and passwords, but signing up has exposed the data of some users to hackers.

When using your credit card to make purchases over the internet, deal only with reputable companies. A secure operating environment is usually indicated by a padlock symbol appearing in the right-hand bottom corner of the website, but be aware that fraudsters can also copy or “spoof” this icon.

Phishing

“Phishing” refers to fraudulent email messages that appear to come from legitimate businesses. These often authentic-looking messages are designed to trick recipients into divulging account numbers, passwords and credit card numbers. Remember that a reputable organisation will not ask you for this information via email or phone. If possible, avoid opening emails from unknown sources.

Most “phishing” emails will not address you by your name because they are blanket emails sent out to thousands of potential targets. “Phishing” emails often try to instill a sense of urgency, claiming your account will be closed down unless you log on or suggesting you need to act quickly to get a security upgrade. Some look quite innocent and can even take the form of weather reports or news events, but they will almost always ask you to click on an active link to see further details. Don’t take the bait – never click on the links in the email even to have a look at them because they may contain dangerous viruses, such as spyware, that can capture your personal details. Delete such emails from your system.

Spoofing

"Spoof" websites that copy the home pages and logos of legitimate financial institutions are an increasing problem. Again, they are designed to capture your personal data for fraudulent purposes. If you have any concerns, contact your financial institution or refer to its website for up-to-date security advice. Users should protect themselves by installing the latest anti-virus software and personal firewalls.

Spyware

Spyware is a hidden enemy within our computer systems. This software can monitor a computer user's private information and steal it through the internet without the user's knowledge. Some spyware arrives as an email and infiltrates your computer, even if you haven't opened an attachment. Your password keystrokes can then be monitored and sent to a third party. Anti-spyware software is available. It works by scanning your computer disks to find any hidden spyware.

Email rip-offs

Some online con artists will email you directly, asking for money or financial details. Be vigilant, keep your radar up and resist the temptation to pass on your private information – once it is out there, there is no way of preventing its misuse. Some rip-off schemes are so notorious that they are known around the world. It's hard to believe people keep falling for them, but they do. They include:

The Nigerian scam: A long-running con whereby fraudsters purporting to be government officials invite individuals via email or letters to participate in a scheme to distribute millions of dollars to needy people in return for a cut of the money. Recipients are asked to divulge bank account details and forward money in "advance fees".

The Spanish lottery scam: Victims receive a letter advising them they have won a prize from the "Spanish Lottery". To collect the prize, they must send money before a certain date to a bank account in Spain to cover the cost of bank fees, delivery and insurance costs.



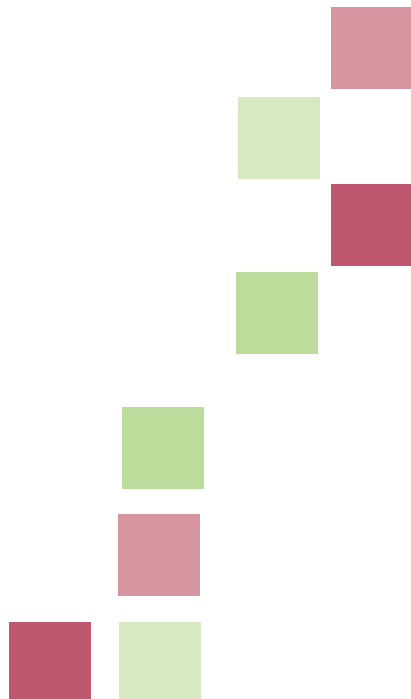
It is a sickening feeling to know that someone could be in possession of your personal financial and passport details. Worse still is a scenario in which they use the data to remove money from your bank accounts or to steal your identity. Cases of ID theft are growing and can result in victims having to prove to authorities and financial institutions that they are, in fact, who they say they are. It might be months or years before victims realise they are being defrauded. Once thieves have your personal details, they can open bank accounts and credit cards in your name, take out loans, or open a mobile phone account. In extreme cases, ID thieves have rented accommodation in other people's names and then not paid the rent – giving the victim a bad credit rating. Internet purchases with unknown companies, failure to check account statements and password laziness can leave you vulnerable. The key to prevention rests in some very simple actions.

Password vigilance

Don't be lazy. Passwords are an important safety tool for a range of financial tasks ranging from EFTPOS, internet banking and ATMs. The temptation is to use a very simple password and to keep it forever – a risky practice that increases the risks of con artists accessing it. It's best not to use passwords that replicate your phone number or date of birth (it's the technology equivalent of leaving the key under the doormat). Create passwords that use a combination of letters and numbers that cannot be easily attributed to you. The longer the password, the harder it is to crack. And change your password regularly (perhaps every 60 days) to foil hackers.

Tips

- Don't be fooled by people posing as landlords, employers or marketers who claim to have a legitimate reason to access your personal details.
- If you live in shared accommodation, or have cleaners, babysitters and the like in your home, don't leave personal details lying around.
- Keep an eye on your purse or wallet ^ they are a goldmine for someone trying to steal your identity. And try not to carry too many credit cards or too much personal information in them.



Who To Contact

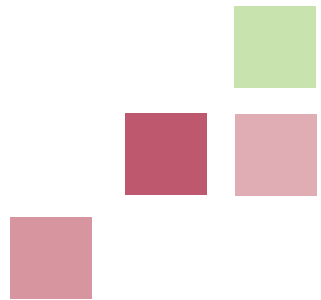
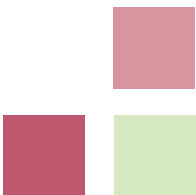
If you think you are a victim of identity theft, you should, first and foremost, contact your credit provider, such as your financial institution, which can monitor activity on your accounts. You should also tell the credit bureau office in your state, and ensure the theft of your identity is registered on its system.

Other institutions to contact include:

- The police service in your state or territory. Officers in all states and territories are being trained to respond to identity crime and significant work is being done to help victims.
- The Australian Crime Commission's identity fraud intelligence facility (www.crimecommission.gov.au).
- Baycorp Advantage (www.mycreditfile.com.au), to let the credit bureau know you have been hit by fraud.

- Australian High Tech Crime Centre (www.ahtcc.gov.au).
- National Legal Aid (www.nla.aust.net.au), which represents each of the eight state and territory Legal Aid commissions across Australia.

The Federal Government has also released a guide to preventing identity theft, which can be found at www.crimeprevention.gov.au under Publications.





www.cu.net.au