

# Theft by fraud

by the QPS Major Fraud Investigative Group

An example of a credit card skimming device installed over the card vent at a bank automatic teller machine. Once inserted over the card area, the victim inserts a card into the automatic teller, believing it is being read only by the automatic teller machine. As the card passes the skimmer, the card is read before entering the automatic teller machine. Usually a secreted camera is recording the key strokes on the auto teller machine to read the pin number.



**A**ccording to the Australian Government, fraud is currently the most expensive category of crime in Australia.

Standards Australia has suggested that the cost to the Australian economy is three billion dollars per year. It warns that both the incidence and the financial impact of fraud is increasing year by year, as is the average financial loss associated with fraudulent conduct.

It is also noted in Standards Australia 2003 publication *2003 Fraud and Corruption Control* that a significant portion of cases of detected fraud are not reported to police for investigation.

Their research indicates that:

- identity theft is becoming the most important fraud related threat within the Australian economy
- Australian organisations are ill prepared to detect and prevent fraud.

Detective Superintendent Kev Robinson from the Queensland Police Service (QPS), Major Fraud Investigation Group said business and the community needed to be better informed about the current trends of fraud to develop strategies to minimise the risk of becoming a victim.

“Globalisation and the advancements in computer technology present ever increasing challenges to law enforcement. Identity theft and computer fraud utilising techniques such as ‘Phishing’ and ‘Trojan Virus’ can be devastating to business and individuals,” he said.

### **General fraud**

Fraud is generally described as gaining a benefit by deception and usually results in financial or material loss to the victim.

There are numerous types of fraud that can be perpetrated on an individual or business. Such frauds include:

- fraudulent investment schemes
- fraudulent property and real estate schemes
- misuse of trust funds by lawyers and accountants
- criminal or unethical behaviour by directors of companies

- insurance fraud
- share market/prospectus fraud
- misuse of power of attorney
- significant employee or employer theft or fraud
- government sector fraud
- arson for financial gain
- cheque fraud
- impersonation
- misappropriation through a variety of representations
- ‘too good to be true’ scams

### **Identity fraud**

Identity theft refers to the theft and use of personal information of an actual person as opposed to the use of a fictitious identity. This can include the theft and use of identifying personal information of someone who is dead or alive.

Identity theft happens in a multitude of ways. It can range from someone using credit cards illegally to make purchases over the Internet or telephone, through to having someone’s entire identity assumed by another person to open bank accounts, take out loans, make a tax return and conduct other business illegally in their name.

In many cases the victim will not know that they have been defrauded for some time. At that point they may have suffered considerable financial loss and their personal credit ratings can be destroyed.

### **Internet theft**

‘Phishing’ is a technique used by criminals to gain personal information for the purposes of identity theft and fraudulent activity. It is most commonly achieved by an email message that appears to come from a legitimate financial institution and in some cases replicates the home page of that business.

These authentic looking messages are designed to lure recipients into divulging personal data such as account numbers, passwords, or credit card details.

“No legitimate financial institution would ever ask you to divulge account and password details in an email message,” said Detective Superintendent Robinson.

“Anyone who receives such a request should not reply to the email or click on any link contained within the message. They should immediately contact the institution by telephone.”

‘Trojan viruses’ are covert computer programs placed on a victim’s computer without their knowledge to enable the perpetrator to access details on the computer from a remote location.

It allows the remote users unrestricted access to the programs, data and security features of that computer. This enables the remote user to control someone’s personal computer and extract and use that information for personal gain.

This invasion of privacy can have a devastating effect on a person’s reputation, business and financial affairs.

“Those businesses or individuals who have effective risk management processes or audit practices in place greatly reduce the risk of becoming a victim of fraud,” Detective Superintendent Robinson said.

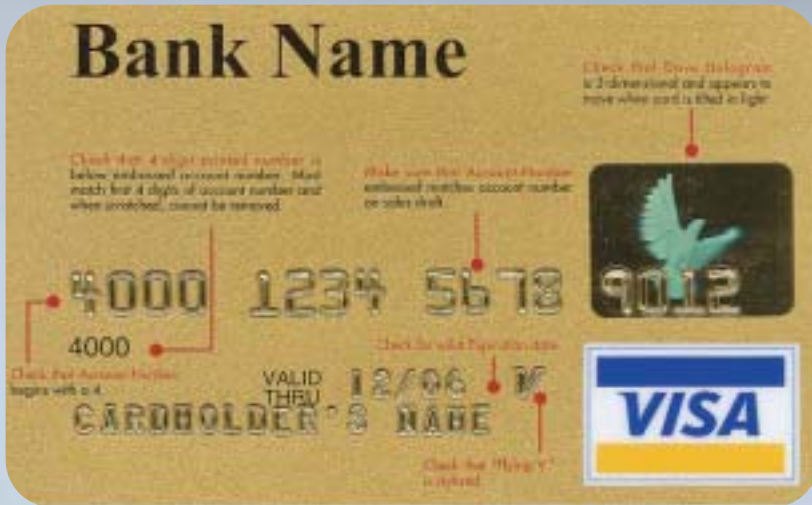
“People should ensure that they have an up-to-date antivirus program and a firewall installed on their computer, which protects the computer while on-line.”

To obtain more information about further preventing Internet or identity fraud or need to report suspected fraudulent activities visit [www.police.qld.gov.au](http://www.police.qld.gov.au) and search under ‘programmes’ then ‘crime prevention’; attend your local police station to report offences or make an inquiry or report all suspected fraudulent activity to Crime Stoppers on 1800 333 000.

Other useful Internet sites include:

- Australian Securities and Investments Commission <http://www.asic.gov.au>
- Australian Competition and Consumer Commission <http://www.accc.gov.au>
- Queensland Office of Fair Trading <http://www.fairtrading.qld.gov.au>

For further information on how the Major Fraud Investigation Group can help you or your business, please contact: Major Fraud Investigation Group on telephone 3364 6622.



Credit card merchants provide educational cards to show retail businesses what security features to look for.



# How to prevent becoming a victim of fraud

## General Fraud

- Develop a healthy trust relationship with your professional financial or legal advisor.
- Store valuable personal documents i.e. Wills, Powers of Attorney, Securities, and Bonds etc in secure places.
- Seek alternate additional professional advice concerning any financial investments.
- Beware of financial investment and taxation minimisation schemes that seem 'too good to be true'.
- Store your chequebooks in a secure location within your residence or business premises.

## Identity Crime

- Check your credit record or banking statements frequently.
- Place passwords on all your important accounts and records.
- Memorise passwords; do not keep the password in your possession.
- Secure your personal information (Passport, birth certificate, etc).
- Don't carry personal information with you unless you need to.
- Destroy personal information before disposal (i.e. shred, cut up expired cards).
- Avoid giving personal information over the telephone, by mail or the Internet.
- Secure your mailbox with a lock. Check contents regularly.
- Check billing and account records carefully for unfamiliar entries.
- Limit the amount of credit you have in your Internet bank accounts.
- Treat with caution any request for your email details for mailing accounts.
- When paying with a credit card at restaurants and general businesses using credit or electronic banking facilities (EFTPOS) always keep the credit card in your sight. (To avoid unlawful skimming).
- When banking at an ATM, familiarise yourself with the ATM and inspect any unusual card reading slots attached to the machine.
- Avoid shoulder surfing (observing you type your password) by other people in the proximity of you at an auto-teller machine.
- When undertaking transactions of people using a credit card, be mindful of the common design and security features. Ensure that the card being used is authentic to the best of your knowledge.

## Computer 'Phishing' and 'Trojan Viruses'

- Always use passwords.
- Update and change your password regularly.
- Do not use automatic log on features that save your user name and password.
- Always log off your computer when you have finished using it.
- Use the latest protection software eg anti virus protection and encryption.
- Use a personal firewall to secure your PC when online.
- Beware of unsolicited emails. Do not follow up or reply. Delete without opening.
- Only conduct business transactions with secure websites eg banks, financial institutions and reputable business institutions.
- Regularly back up the information in your computer. Wipe the hard drive if you sell or dispose of your computer, ensuring that all files you created are rendered unrecoverable.
- Avoid using computers that are available to the general public to access your private personal information as your password and credit card details may be compromised.