



AUSTRALASIAN IDENTITY CRIME POLICING STRATEGY 2003-2005

In the rapidly developing global e-commerce environment, the ease and speed with which identity crime can occur has increased dramatically.

As a result, the Australasian Police Commissioners have undertaken the development of a policing strategy to address the issue.

The purpose of the strategy is to prevent and reduce identity crime and to assist the victims of "identity theft".

The focus areas are:

- Prevention
- Victim Assistance
- Partnerships
- Education and Capability
- Resources and Capacity
- Regulation and Legislation

For a full copy of the strategy please visit www.acpr.gov.au



WHO TO CONTACT

If you have information concerning identity crime or identity fraud you should contact:

If you believe that you, or your business, have become a victim of identity crime, or that your name or someone else's has been used for criminal purposes, you should report the matter immediately to the police.

USEFUL WEBSITES

- www.acpr.gov.au
- www.accc.gov.au
- www.ahtcc.gov.au
- www.usdoj.gov/criminal/fraud/idtheft.html
- www.consumer.gov/idtheft/
- www.idtheftcenter.org/facts.shtml

June 2004



IDENTITY CRIME

WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME

In the course of a busy day, you may write a cheque, call home on your mobile phone, apply for a new credit card or order tickets online.

Chances are you don't give these everyday transactions a second thought. But someone else may.

There is a new variety of crook called a identity thief. His or her stock in trade is your everyday transaction. Each transaction requires you to share personal information whether it be your credit card number, home address, telephone number or social security number.

An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft.

This brochure has been developed to provide you with information on identity crime, how to prevent it and what to do "when bad things happen to your good name."

IDENTITY CRIME

Identity Crime broadly describes criminal activity in which a perpetrator utilises a false identity in order to facilitate the commission of a crime. Identity crime can underpin and facilitate a range of crimes including people smuggling, drug trafficking, money laundering, paedophilia, terrorism and murder, but is most commonly typified by identity fraud.

IDENTITY FRAUD

Identity Fraud generally involves the gaining of money, goods, services or other benefits through the use of a false identity and can include, but is not limited to, the following types of criminal activity:

- Counterfeiting and "skimming" of credit cards;
- The use of stolen credit cards or credit card numbers;
- Fraudulently obtaining money, loans, finance and credit;
- Fraudulently obtaining benefits, pensions or entitlements;and
- Evading the payment of taxes, levies or other debts.

IDENTITY THEFT

"Identity theft" is the a takeover of a person's identity by utilising stolen personal information, or fraudulently obtained, forged or stolen identity documents.

Identity theft often results in the takeover of a victim's existing bank accounts or by the fraudulent operation of new accounts opened by the perpetrator in the victim's name.

Identity theft brings with it additional problems of victimisation for the person whose name has been "stolen". These problems centre on the victim undoing the damage that has been caused to their name and reputation.

Many victims need to expend large amounts of time and resources convincing banks , financial institutions and other agencies that they were not responsible for the fraudulent activity that occurred in their name.

Many victims have also found difficulty in restoring their credit rating to what it was prior to the theft of their name. In instances where the name stolen is that of a deceased person, the surviving relatives effectively become the victims and can experience similar difficulties and associated emotional trauma.

INDIVIDUALS

- Security of personal and business information is critical. Criminals commonly rummage through the rubbish bins looking for personal identifying data that they can steal and use to commit fraud and other offences in your name.
- Take time to shred or destroy old bank statements, credit card bills, utility bills or other documents to prevent this material falling into the hands of criminals.
- Be careful towhom you give personal information. If you have to reveal personal information, ask some questions about the security of the information and be very cautious giving out any information over the phone or Internet unless you know who you are dealing with.
- Guard your mail from theft by securing your letterbox. Criminals value your mail and will use it to commit fraud with your accounts or open loans or credit in your name.
- Minimise your identification and the number of cards you carry in your wallet to what you actually need.
- Check your bank and credit card statements to make sure there are no unauthorised transactions—this may be the first sign someone has stolen your identity.

ORGANISATIONS

- For businesses, internal documents like cheques and letterheads should be distinctive and include some type of security feature to deter forgery.
- Credit Card transactions can be problematic for merchants, particularly phone and Internet credit card orders, where the card is not produced. Criminals often use credit card numbers without actually having possession of the card.