

In the course of a busy day at work, you may write a cheque, call a distributor on the mobile phone, apply for a new business credit card or purchase merchandise online.

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

There is a new variety of offender called an identity thief. His or her stock in trade is your everyday transactions. Many transactions require you to share sensitive information about your business (or your customers).

An identity thief can obtain some piece of your business' information (such as its name or financial details) and use it without your knowledge to commit fraud or undertake some other activity. Both small and big business can be the victim of identity crime.

This brochure has been developed to provide you, as a business owner or manager, with preliminary information on identity crime, how to prevent it and what to do "when bad things happen to your business' good name".

IDENTITY CRIME

Identity crime broadly describes criminal activity in which someone uses a false identity to commit crime.

Identity crime most commonly relates to fraud, but it can include a range of crimes including people smuggling, drug trafficking, money laundering, paedophilia and terrorism.

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 the following types of criminal activity:

- Counterfeiting and "skimming" of credit cards;
- The use of stolen credit cards or credit card numbers;
- The use of "ghost" websites to elicit customers' personal information (known as "phishing");
- Fraudulently obtaining money, loans, finance and credit;
- Fraudulently obtaining benefits, or entitlements; and
- Evading the payment of taxes, levies, or other debts.

IDENTITY THEFT

"Identity theft" often results in the takeover of a victim's existing bank accounts or the fraudulent operation of new accounts opened by the perpetrator in the victim's name. A 'victim' could be you as an individual, your business or your customers.

Identity theft brings with it additional problems for the victim whose name has been "stolen". These problems centre on the undoing of the damage that has been caused to name, reputation and financial well-being.

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

Many victims have also found difficulty in restoring their business' credit rating to what it was prior to the theft or misuse of its name.

BUSINESSES

A "plain English" guide has been developed for businesses and individuals to protect them from identity fraud by the Macquarie Bank in conjunction with the Fraud Squad of the New South Wales Police.

To view this guide visit:

www.macquarie.com.au/au/about_macquarie/media_centre/20030227.htm.

Some of their tips and others include:

- Keep all sensitive business information, such as tax records and other financial information, in a secure place. Shred all unwanted sensitive documentation (both your own and that of your customers) and ensure secure disposal.
- Secure business cheque books and stationery away from the reception desk.
- Use a locked mail box to send and receive all mail. Ensure that the mail box is capable of holding the quantity and size of the mail you normally receive.
- Have your accounts department or finance person monitor and validate each account statement and check the credit reports of your business on a monthly basis to make sure there are no unauthorised transactions.
- Never divulge business financial information, including credit card numbers and PIN numbers, to external parties unless you know who they are. Never provide this information on the Internet unless you are sure it is a secure site.
- Train your staff to deal appropriately with your customers' personal information and never divulge customer information inappropriately to external parties.
- Ensure you have appropriate security on all of your computers. When disposing of computers, ensure that the hard drives are permanently erased or destroyed.
- Ask for more identification if you suspect another party of identity fraud. Be wary of individuals who, for whatever reason, are unable to provide identifying information or have a lot of reasons why you should not follow normal business procedures.
- Most importantly, report all suspected frauds or the misuse of your business identity to the police and your merchant processor immediately.



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 you should contact your local police station.

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.acc.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 BUSINESS' GOOD NAME