



AUSTRALIAN BANKERS' ASSOCIATION INC.



ASIC

Australian Securities & Investments Commission

Immediate Steps

If your identity has been stolen, it's essential that you act quickly to minimise the damage already caused and to limit the possibility of future problems.

Step 1

Contact your banks, other financial institutions and card issuer to advise them of the disputed transactions or other concerns you may have. This may involve:

- Stopping payment of lost or stolen cheques
- Changing PINs and/or passwords
- Discuss with your bank whether there is a need to close your current accounts and reopen new ones.

Ensure that you advise the banks, financial institutions and card issuers of all accounts that are involved.

Step 2

Also report identity theft to your local State or Territory Police – you may be asked to undergo police routines of photographing and fingerprinting to establish that you are not the same person as the person who stole your identity and used it fraudulently.

Step 3

Contact the *Credit Reporting Agency*. Tell them that you believe you have been compromised by identity theft and request a file note to be placed on your file. You may also want to obtain your file to:

- Check your credit file carefully for unauthorised entries and look for accounts that have been opened in your name, or unauthorised changes to your existing accounts. If you find fraudulent applications or overdue account listings on your report, you will need to contact the companies that have listed them so that they can investigate the matter and have the fraudulent entries removed from your credit history.
- Request a further report in a few months time to ensure that no further fraudulent activity has occurred. If there have been further entries, then carry out the same actions as detailed previously.

Important Note: This fact sheet gives information of a general nature and is not intended to be relied on by readers as advice in any particular matter. We suggest that you consult your financial planner on how this information may apply to your own circumstances.

Step 4

Contact your local Post Office to check if your mail has been diverted to another address.

Step 5

Document (time, date, contact person and telephone number, and advice received) the timing and nature of conversations in reporting the incidents to the various agencies, including the police.

Step 6

Contact any relevant government agencies or departments, for example Centrelink or the Australian Passport Office.

What documents could I need?

Each of these organisations may ask you to provide written documentation to support your case and to establish that you are not liable for any debts accumulated in your name. You may be required to complete a statutory declaration and/ or a statement of Fraudulent/ disputed accounts.

How long can the effects of identity theft last?

It's difficult to predict how long the effects of identity theft may linger. That's because it depends on many factors including the type of theft, whether the criminal has sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit file.

If you've suffered from identity theft, you should monitor your credit files and other financial records for several months after you've discovered the crime. It's also worthwhile reviewing your credit files once every three months in the first year of the theft, and once a year thereafter.

(Fact Sheet continues on next page)...

Electronic Funds Transfer (EFT) Code – what do to about unauthorised transactions on your account

What is an EFT code?

The EFT Code (the code) is a voluntary code however all banks, building societies and credit unions that provide retail EFTPOS and ATM services or telephone or internet banking subscribe to it.

Why is it important?

The code provides protections for consumers by requiring that key disclosures are made and privacy protections are in place. Importantly, the code sets down the rules for resolving disputes about unauthorised transactions.

If you find a charge on your credit card statement that you do not agree with (unauthorised or irregular), notify your credit card provider immediately.

Will I be out of pocket?

Usually, in these circumstances, your credit card provider will reverse the transaction immediately. The provider then seeks a chargeback from the merchant's bank. Unless the merchant can establish that you, or a secondary cardholder, did in fact receive the goods or authorise the transaction, the reversal will remain in place.

Time limits do apply to reversing transactions, so always check your credit card statements carefully and take immediate action if you cannot account for a transaction that you see.

Before you request a reversal, double check that the transaction can't be matched to one of your credit receipts, as some merchants appear under a different name when they are listed on your credit statements. For example, you may have purchased a rake from Greg's Garden Gadgets, but the transaction may appear on your credit statement under a different name, such as G Smith Trading Co.

To find out more about the Code and how it protects you as a consumer, go to the Australian Securities and Investments Commission's (ASIC) consumer website, FIDO, at <http://www.fido.asic.gov.au/>, or call ASIC directly on 1300 300 630 to request a copy.

December 2006

Web: www.protectfinancialid.org.au Phone: 02 8298 0417 Fax: 02 8298 0402