

August 23, 2013 Release # 229

-- Begin Transmission --

## What You Need to Know to Avoid Identity Theft - Final Part

## What to do if you become a victim

If you discover that your identity has been compromised or stolen, take immediate steps to address the situation.



If you think someone has gained access to your online account, telephone banking account or credit card details - Call your bank immediately, so they can suspend your account. The appropriate telephone number should be on the back of your ATM or credit card, or on an account statement. Alternatively, you can look up the correct number in the phone book. DO NOT contact the company using details that appear in emails or on websites that you are suspicious of—they will probably be fake and lead to a scammer. Alerting your bank immediately can limit the amount of money you are liable for. Credit card companies may also be able to perform a 'charge back' (reverse the transaction) if they believe that your credit card was billed fraudulently.

## If you have sent money to someone that you think may be a scammer

- If you sent money through an electronic funds transfer (over the internet), contact your bank or immediately and ask them to cancel the transfer. They may be able to stop the transfer if it has not already been processed.
- If you sent a cheque, ask your bank to 'stop' the cheque. You must do this before the cheque is drawn on (cashed in by a scammer).
- If you sent money through a wire service, contact the wire service immediately and ask them to stop the transfer (you will need to be very quick).



If you have been scammed using your computer - Chances are the virus or other malicious software is still on your computer. You should run a full system check using a reliable virus checker. If you do not have this software and other protections like a firewall installed on your computer, you should do so (a software professional can help you decide what is best). The scammers may have gained access to your online passwords so, after you have cleaned up your computer, you should change these as well.

File a Police Report - You may also report the incident to your local police department and the National Bureau of Investigation as well.

-- End of Transmission -

Information Security: It's a Shared Responsibility

REFERENCE(S): http://www.scamwatch.gov.au/

INTERNAL USE ONLY: For circulation within the PJ Lhuillier Group of Companies only.

Document Code: 2013ICT\_15SECA032