Tomorrow MONEY

Spotting and recovering from identity theft

What is identity theft?

We all have an identity – it simply means who we are. Our name is part of our identity and it's linked to lots of things we may use in everyday life, like our driver's licence, passport, our banking accounts and our Medicare and Centrelink information.

Sometimes scammers steal this information so that they can take people's money. This is called identity theft. It can happen in a number of ways, such as:

- Someone tricking a person into handling over personal information, like credit card details.
- Someone hacking into a computer or phone to steal information.
- Someone creating a pretend profile to convince a person to hand over information.
- A bot using a computer program to get into private files.

SIGNS OF IDENTITY THEFT

Here are a few things to watch out for and some actions to consider:

WARNING SIGN	WHAT TO DO
A text or email asks you to click a link – but you don't recognise it.	**Don't open** the message if possible. If you do, delete it without clicking the link.
Someone you don't know calling saying your account has been hacked into or breached and then asking for private information.	**Hang up** or ask for a number you can call them back on. If they don't provide the number, they are likely not who they say they are.
Someone you don't know tries to befriend you on Facebook or Instagram	**Ignore** or delete the request.
Money is missing from your bank account or you don't recognise spending something that has shown up on your statement.	**Contact your bank** to ask about it.

First Nations FOUNDATION

AN EXAMPLE:

Rob's Mysterious Spending

Rob was doing some online banking when he noticed that $54.00 had been taken out of his account on Tuesday, when he was home with the flu. Rob didn't recognise the name of the company which took the $54.00, so he decided to call his bank.

He rang the bank's main line and explained, "There is a charge of $54.00 in my account that I don't recognise. Can you tell me where it was spent?"

It turned out, a scammer had spent the money in South Africa. Once the bank realised that Rob had not been the one to make the purchase, the bank put a stop on the card and sent out a new one.

WHAT IF MORE MONEY IS TAKEN?

In the example scenario, the scam was noticed relatively early and before much money had been spent. Unfortunately, sometimes these scams aren't known about until more money has been taken. If this happens, it can be upsetting, but help is always available. See the numbers below.

WHERE TO GET HELP

If you are upset, distressed or worried, you can call **Lifeline on 13 11 14.**

If your identity has been stolen, there are a number of places to report it:

- If the scam relates to **Centrelink, Medicare, Child Support or MyGov**, you can call the Services Australia Scams and Identity Theft Helpdesk on 1800 941 126
- IDCARE can help to **recover your identity for free.** Visit idcare.org or call 1800 595 160.
- Apply for a **Commonwealth Identity Theft Victims Card.** This can help to let other government agencies know that you don't have the paperwork you need to prove your identity, but are setting it up again. You can apply via homeaffairs.gov.au
- The **ACCC's Scamwatch** keeps an eye on scams, collects reports and provides information to other agencies which can shut the scams down. Visit scamwatch.gov.au
- If you feel comfortable doing so, you can report it to the police on 131 444.

Sources: ACCC's Scamwatch; homeaffairs.gov.au.