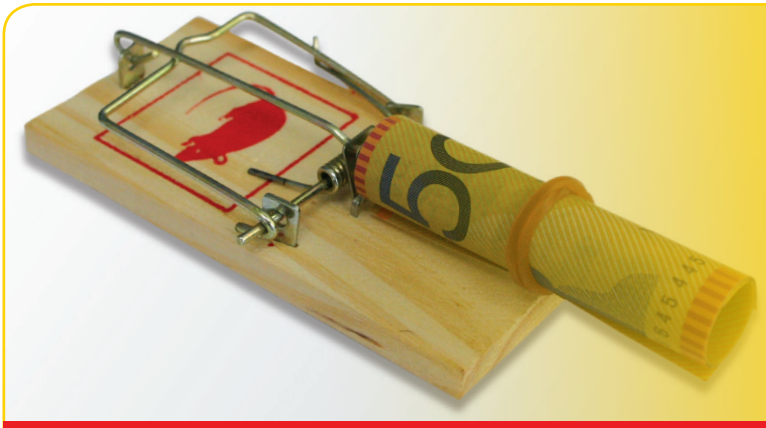

FLIP

(Financial Literacy in Practice)

February 2015

IDENTITY THEFT

TEACHER NOTES

OVERVIEW

This resource complements the material in Operation Financial Literacy. It has been written to address current issues which specifically relate to Module 11: **Scams – Don't be caught out.**

Module 11 aims to provide students with an overview of all aspects of scams and how to effectively respond to them.

TEACHER NOTES

FLIP POWER WORDS

authentication	fabrication	indemnity	theft
encryption	fraud	shoulder surfing	utilities
evidence document	identity	skimming	

Before students begin the activities, some classroom discussion and research on definitions, power words and the likely outcomes of identity theft is advised.

1. To introduce this activity, first discuss and distinguish the phrases "identity theft" and "identity fraud" (which is the result of identity theft). The following definitions are from the 2013 Crime and Justice Statistics on the ABS website:

   IDENTITY THEFT

   This involves the theft and fraudulent use of personal details or documents such as a driver's licence, tax file number or passport to conduct unauthorised transactions including conducting business or opening accounts in another person's name or otherwise using a person's identity without permission.

   IDENTITY FRAUD

   Identity fraud involves the theft of personal details without a person's consent. The person's name, date of birth, address, financial details or other personal details are then used to engage in fraudulent activities, such as conducting business, purchasing goods, withdrawing cash, opening accounts, taking out loans or avoiding criminal liability. This comprises of identity theft and credit or bank card fraud.

Financial Basics Foundation

2. Encourage students to investigate some different types of identity crimes. It may also be useful to discuss the meaning and implications of the FLIP power words. The following definitions are sourced from this website: http://www.protectfinancialid.org.au/Jargon-buster/default.aspx

   Identity – encompasses the identity of natural persons (living or deceased) and the identity of companies.

   Identity crime – can be used as a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity or a stolen/assumed identity to facilitate the commission of a crime(s).

   Identity fabrication – can be used to describe the creation of a fictitious identity.

   Identity manipulation – describes the alteration of one's own identity.

   Shoulder surfing – usually happens at ATM machines or public phones. Criminals may watch you from a nearby location, or behind you in a queue, as you key in your PIN. They may also listen in on your conversation if you give your credit card number over the phone, for example, when making a hotel reservation or booking a rental car.

   Skimming – is the unauthorised copying of information stored on the magnetic strip of a credit card. This information is used to create a 'cloned card', which is then used for fraudulent transactions in retail outlets or on the internet. The stolen details can also be used for identity theft.

3. Once an identity has been stolen it can be almost impossible to recover. Victims may have problems for years to come. Brainstorm with students about the types of fraud which could be committed once thieves have access to personal information. Further information on this can be found here: http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Protecting%20Your%20Identity%20booklet%20%20What%20Everyone%20Needs%20to%20Know%20.PDF

   Potential kinds of fraud that could be committed using personal identity include:

   - tricking banks or financial institutions into giving access to money and other accounts
   - opening new accounts and accumulating large debts (which will ruin the credit rating and good name of the victim)
   - taking control of bank accounts by changing the address for credit card or other accounts so that statements are not received (The victim may not even be aware that there is a problem)
   - opening a phone, internet or other service account
   - claiming government benefits
   - lodging fraudulent claims for tax refunds, thereby preventing the victim from being able to lodge a legitimate return
   - using the victim's name to plan or commit criminal activity
   - embarrassing or misrepresenting the victim, such as through social media.

SOLUTIONS TO ACTIVITIES

ACTIVITY 1: What do thieves want?

CATEGORY A (evidence of the legal existence of name and date of birth)

- Passport
- Driver's licence
- Birth certificate
- Australian citizenship certificate
- Birth certificate or birth card

CATEGORY B (evidence of the use of name in the community)

- Medicare card
- Centrelink card
- DVA card
- Debit or credit card
- Educational institution student identity card

CATEGORY C (evidence of residential address)

- Motor vehicle registration papers
- Motor vehicle insurance papers
- Property rates notice
- Property lease agreement
- Home insurance papers
- Utilities bills
- Bank or credit card statement

SOLUTIONS TO ACTIVITIES (continued)

ACTIVITY 2: A nasty surprise

Whilst some of the items stolen in this scenario have monetary value, or might allow a thief to gain access to other physical items of even more significant value (e.g. credit cards and house keys), the focus of the activity is for students to restrict the investigation to sources of information which might lead to theft of identity.

ITEM/DOCUMENT	INFORMATION WHICH COULD BE USED FOR IDENTITY THEFT
Mobile phone	• Phone numbers, email and physical addresses, birth dates for your contacts • Passwords, codes and PINs • Sensitive corporate information about your employing organisation
Computer (tablet, laptop, etc)	• Remembered passwords for banking and other accounts • Saved documents, statements, etc. containing personal details, passwords and PIN details • Email containing personal details • Secure information and documentation relating to your employer • Access to your social media accounts
Driver's licence	• Personal details • Photo ID
Credit card	• Credit card number • Security code (CVV or CVC) • Your name
Debit card	• Debit card number • Your name
Medicare card	• Medicare card number • Your name
Health insurance card	• Card number • Your name
Employee or student ID card	• Card number • Your name
House keys	• Access to your home
Work keys	• Access to your place of employment
Key to your post office box	• Access to your mail, name and address
Portable GPS navigation device	• Access to your home and work addresses
Opener for house gate or garage door	• Access to your home
Opener or access card for work doors or work garage	• Access to your place of work
Vehicle registration papers	• Your name and address • Information about your motor vehicle
Vehicle insurance papers	• Your name and address • Information about your motor vehicle
Motor vehicle assistance card	• Your name and address • Information about your motor vehicle
Health club card	• Physical after-hours access to your gym
Library card	• Account number • Your name
Store loyalty cards	• Your name
Passport	• Evidence of your legal existence • Date of birth
Birth certificate	• Your date of birth
Bank statements	• Account numbers • Evidence of residential address
Utilities bills	• Evidence of residential address
Taxation documents	• TFN (Tax File Number)

SOLUTIONS TO ACTIVITIES (continued)

ACTIVITY 3: Act quickly

Students use this website to find the correct order of steps:
http://www.protectfinancialid.org.au/Immediate-steps/default.aspx

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.
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 one who stole your identity and used it fraudulently.
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.
4	Contact your local Post Office to check if your mail has been diverted to another address.
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.
6	Contact any relevant government agencies or departments, for example Centrelink or the Australian Passport Office.

ACTIVITY 4: Don't be a victim

This extension activity is useful for highlighting some key issues associated with identity theft. The time needed to complete the activity (and its complexity) depends on the medium chosen.

This website links to some useful fact sheets on how to avoid identity theft:
http://www.protectfinancialid.org.au/Useful-factsheets/default.aspx

Financial Basics Foundation