

Protecting yourself
and your loved ones
from financial abuse.



Introduction.

Financial abuse is more common than you would think with thousands of cases occurring across Australia every year. It affects people of all cultural, financial and social backgrounds. That's why we are here to help with the tools and information on how to help keep you safe.

If you feel like you may be particularly vulnerable due to your reliance on assistance from carers or support workers, from deteriorating mental or physical health, or even from social isolation - it's important to be aware of the ways in which your financial wellbeing could be abused by others. Equally if you are a carer, supporter or relative of someone who could be experiencing vulnerability, it's important to know how to best watch out and protect those who depend on us. Understanding how to identify the signs of financial abuse can help keep you safe and protect your financial independence.

Common forms of financial abuse.

There are many forms of financial abuse.
This brochure covers some of the most common:

- Manipulation
- Scams
- Fraud

We're here to help.

 132 032

What is financial abuse?

Financial abuse occurs when a trusted individual manipulates or compromises the financial decision-making of an individual. Often involving misusing or taking control of their money, financial resources, property or assets, without their knowledge, consent or understanding.

Financial abuse can take many forms and usually consists of purposeful actions over a period of time, rather than a single event.

A 'financial abuser' can be someone you hardly know or someone you have known all your life. They could be family members, friends, acquaintances, a neighbour or strangers who befriends you. They may also be professionals or caregivers employed to help you. This brochure outlines some of the things you can do to help prevent financial abuse.

For example: A family member forcefully has an elderly person appoint them as a power of attorney so they can transact on their account for their own interests.

What are scams?

A scam occurs when an individual is manipulated or misled regarding the benefit or purpose of a transaction and willingly transfers money.

For example: A fake Australian Tax Office call threatening arrest if a tax debt is not settled immediately.

What is fraud?

A fraud occurs when the transaction or method of loss occurs without the individual's authorisation.

For example: Your credit card details being stolen and used to purchase goods overseas.

Protecting those you love or support from financial abuse.

Financial abuse can happen to absolutely anyone but there are some groups who are particularly vulnerable. People who depend on family, friends and support workers for their day-to-day care or social contact have the greatest risk of financial abuse.

There are no circumstances in which financial abuse is acceptable, so if you think this might be happening to you, don't be afraid to seek help. See page 37 for details.






You can help.

As a carer, supporter or relative of someone experiencing vulnerability, there are steps you can take to help protect them from financial abuse.

You should:

- Look out for the warning signs on page 10.
- Help set up support networks that include independent people without conflicting interests in assets.
- Report instances of abuse, fraud and scams to the bank and or relevant government departments on page 37.
- And if you are appointed under a power of attorney, ensure you understand your own obligations and duty of care in managing the affairs of others.



Joan's story of financial abuse.

Joan suffers from Parkinson's and in preparation for her declining condition, her son was appointed her power of attorney to look after her banking. Joan's son and his wife were eager to purchase their first home, but had been struggling with saving for the full deposit.

Upon becoming aware of his mum's high account balances he decided to borrow some money for his deposit by withdrawing funds in branch. He believed he could simply pay it back later or not worry about it at all, as the money would come to him eventually.

Joan's son went into his local branch to request a cash withdrawal to deposit into his account.

The Bank Manager declined the transaction recognising that her son's role as her attorney was a potential conflict as he had a duty to act in her interest and not to obtain a financial gain.

The Bank Manager then contacted Joan to discuss the transactions with her and suggested she obtain independent legal advice on how to protect her finances.

Warning signs.

Some of the signs that financial abuse could be happening to you or somebody you know are:

- Unauthorised transactions, withdrawals and transfers made from accounts and charged to credit cards.
- Coercion involving alterations to the will, power of attorney or enduring power of attorney.
- The appointed power of attorney not following directions or acting in the interest of the individual to whom they provide care.
- Forged signatures on cheques, bank accounts or legal documents.
- Unpaid bills, despite assigning that responsibility to a trusted person.
- An absence of mail, particularly delayed or missing bank statements.
- Threats of isolation or actualised isolation from friends and family if the financial abuser's demands are not met.
- Stolen or unpermitted seizure of assets, property or possessions.
- Feelings of guilt and obligation if the individual withholds financial assistance.
- Irregular and unusual spending patterns on the victim's account.
- Large, unexplained transactions or transfers to family/third parties.
- Limited ability or means to prove that financial abuse is occurring.
- The individual lacking awareness of their financial situation.
- Feeling pressured into being a guarantor to a loan without fully understanding obligations.



Build your support network.

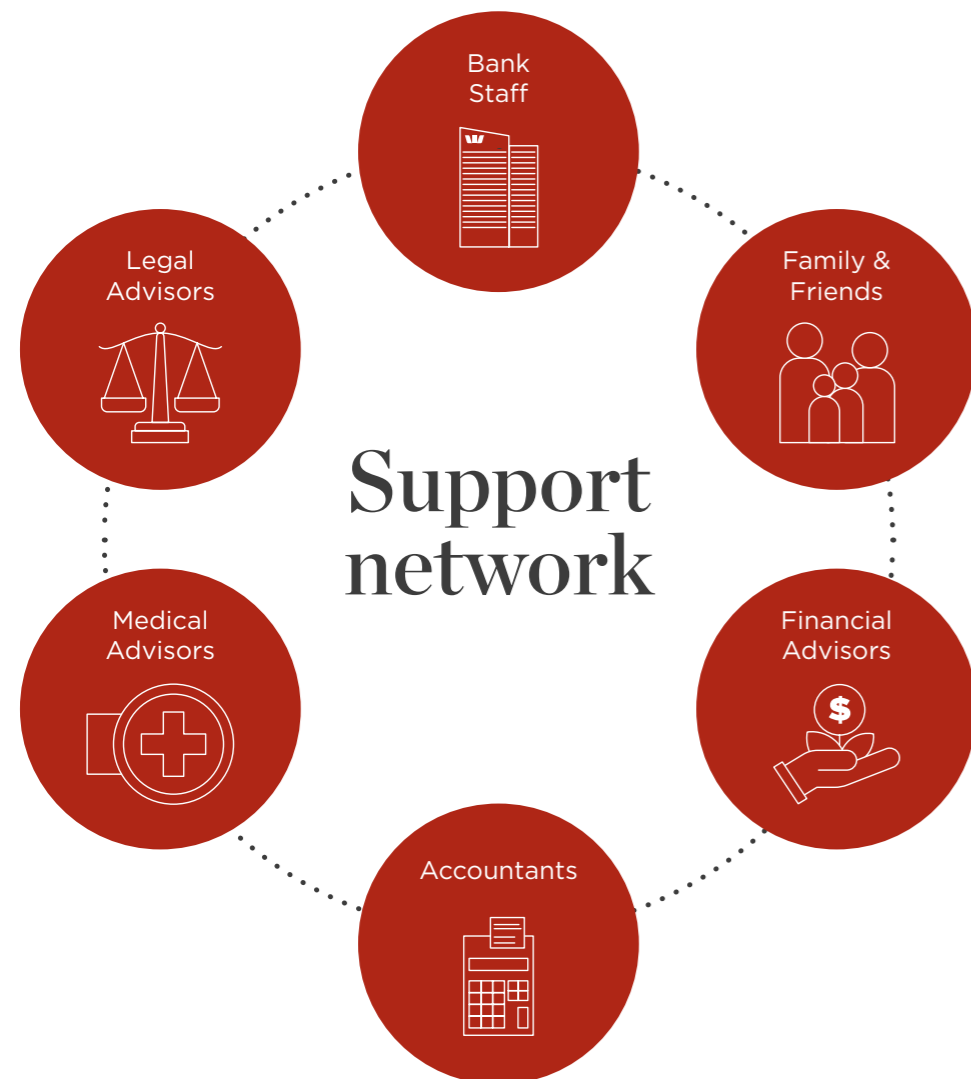
To protect your financial future, set up the right support networks, appoint appropriate third-party representatives and have all the correct documentation in place.

This could include, where appropriate, establishing a power of attorney, third party authorisations and an up-to-date will.

This network needs a contingency plan for support, should something not go as intended.

Ensure your support network is trusted, has the right values and capabilities to help you and has no conflict of interest. It's good to have more than one person in your network.

People you could consider are:



Protect yourself from financial abuse.

- Talk about financial matters with trusted family and friends.
- Keep track of your finances by checking your bank statements regularly to make sure there have been no unauthorised transactions. Talk to the bank if there are any surprises.
- Open your own mail.
- Stay in touch with the people you trust and care about.
- If you lend money to someone, set up a repayment plan, record the signed terms of the loan which should include a repayment plan.
- Never sign a document or make a big financial decision unless you understand the terms and what your obligations are and if you're not sure, seek professional advice.
- Ensure you never share your banking log on details, passwords, security codes, or pins with anyone even if they claim to be from the bank, or a close friend/family member.
- Actively monitor your transactions and statements regularly and talk to the bank if there are any surprises.
- Set up the right support networks and have all the correct documentation in place to protect your financial future.
- Ensure you have an up-to-date power of attorney and send certified copies of important documents to a trusted person.



Scams.

Scams are a form of financial abuse that unfortunately, is on the rise in Australia.

Australians lost



\$489.7 million

to scams in 2018.

And according to a 2019 ACCC report,



48% of all reported scam losses

happened to those over 55 years of age.

These are losses reported to the government and do not include:

- Current victims unaware that they are being scammed.
- People who have been emotionally impacted and decided not to report.
- And people who are unaware of how or where to report scams.

Common scams.

Scammers are very clever and very opportunistic. If you or someone you know, have ever been impacted by a scam, you're not alone.

Here are some common scams to look out for:

Relationship and Romance scams

Scammers often take advantage of people looking for relationships. Once they've gained trust, they begin requesting money, gifts or personal information.

They may:

- Fabricate profiles on dating websites or social media.
- Impersonate professional services such as a nurse or carer.

In 2018 females reported losing \$19.5 million to relationship and romance scams. Dating and Romance scams are the most reported of all the scams.

Investment scams

Scammers offer false opportunities and investments with the promise of high returns.

Scamwatch reported investment scams are the top scam type when it comes to financial losses to customers.

Remote access scams

A scammer attempts to persuade you into giving them remote control over your personal computer. Doing this can provide them with access to financial or personal information that you may have assumed was stored securely.

Threat and penalty

Scammers impersonate reputable organisations, using urgency, threats and intimidation to obtain your money. Calls claiming to be from NBN and the ATO are common examples of threat and penalty scams.





Mark's story of a Romance scam.

Mark met Maureen online. Maureen lived overseas and they had never met face to face, but within four months, they were engaged.

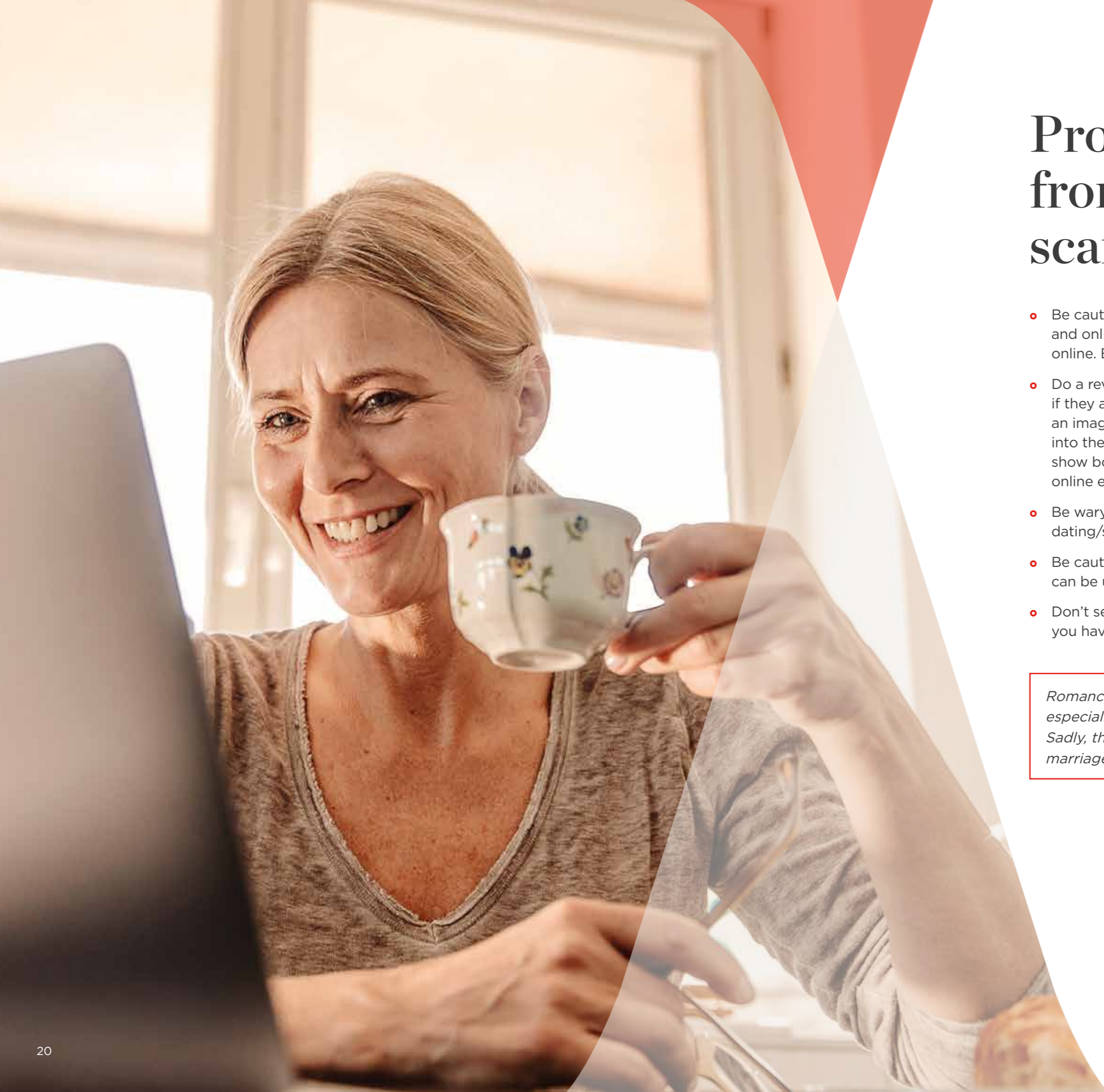
Maureen then explained that she was involved in a serious accident and urgently needed money for medical bills.

Mark wanted to help and completed a number of transfers online totalling \$120,000. However, once Maureen knew that Mark had drained most of his life savings, she ceased contact with him.

At that point, Mark realised something didn't seem right and he called the bank about recovering those funds.

The bank informed Mark that it was a potential scam, so they escalated, reported and reviewed it. Unfortunately, this time it was too late. Maureen had already withdrawn all the funds in cash, making them unrecoverable.

Given Mark provided Maureen with significant personal and online banking details, his online and telephone banking were locked and his account frozen. Mark changed his passwords and added extra security to his profile to help ensure his finances were protected in the future.

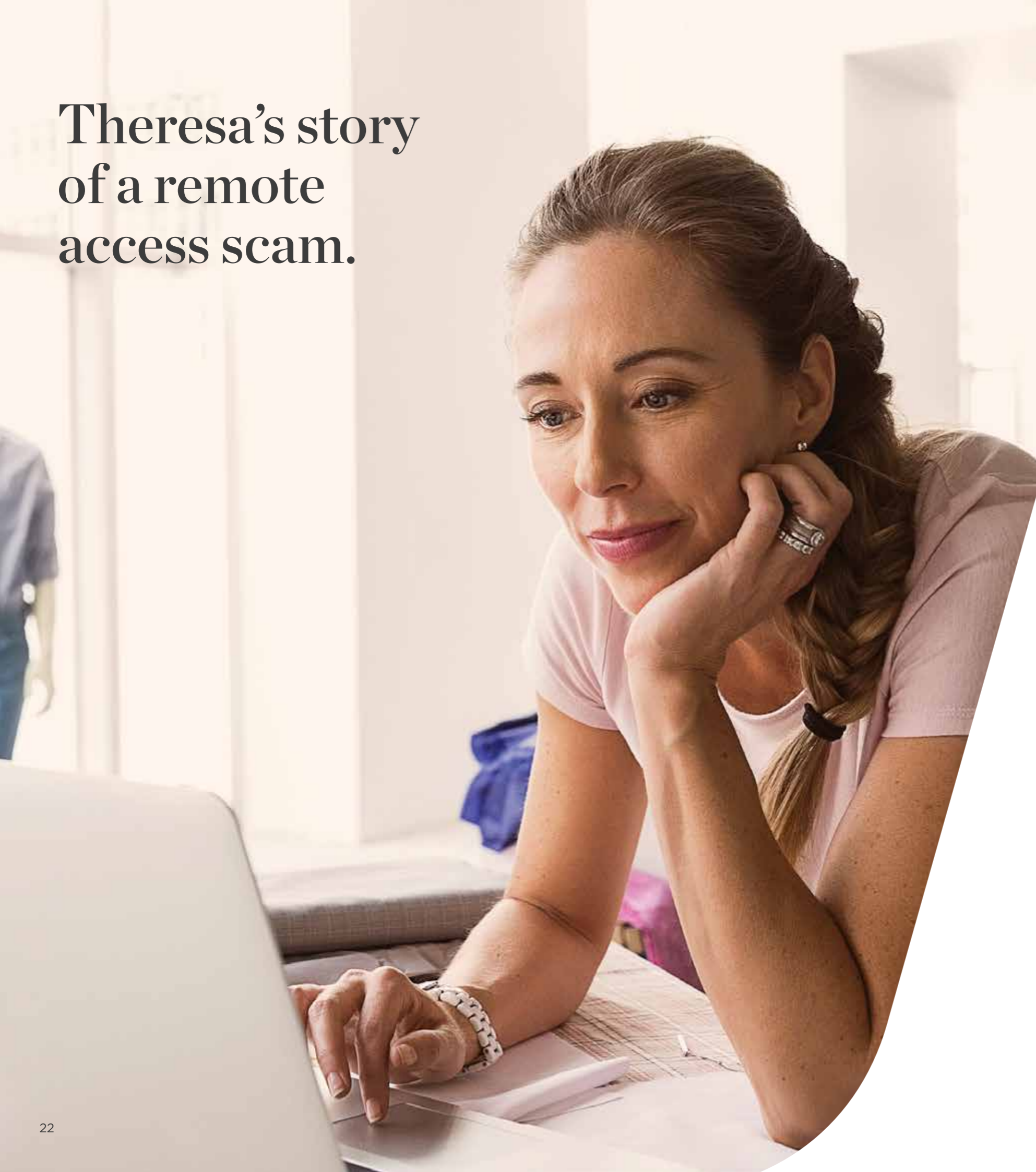


Protect yourself from romance scams.

- Be cautious of unknown “friends” when using the internet and online services. Not everyone is who they say they are online. Be vigilant about what you share.
- Do a reverse image search of your new connection to see if they are who they say they are. You can do this by uploading an image from your desktop, tablet or mobile phone directly into the Google image search bar. The search results will show both duplicates, and similar images that may be online elsewhere.
- Be wary of people who wish to contact you outside of the dating/social media site after just a few contacts.
- Be cautious of sharing intimate photos or videos as these can be used against you for financial gain.
- Don't send money or provide your personal details to someone you have only interacted with online or via the phone.

Romance and friendship scams can happen to anyone, especially at times when you feel lonely or vulnerable. Sadly, this often occurs following the breakdown of a marriage or the loss of a loved one.

Theresa's story of a remote access scam.



Theresa received a call from someone impersonating an NBN worker. The caller advised Theresa that they were installing NBN in her local area and that they required her to complete some actions to activate her service.

Theresa was expecting a call from NBN and followed the instructions to download software and accepted all screen prompts that were presented to her.

Theresa was asked to log onto online banking to make the first payment to ensure that the service will be activated.

The next day, Theresa noticed her account was missing \$10,000 and went to the branch to investigate.

The software that Theresa had installed on her computer was a form of 'remote access software'. This allowed the Scammer to take full control of her computer, including viewing her browser and logging her keystrokes when she signed into online banking and other websites, therefore having access to all her account login information.

Protect yourself from remote access scams.

- Do not download or install remote access software to your computer.
- Do not share your account login information with anyone, including security codes, passwords or SMS verification codes.
- Keep antivirus software up to-date on all your devices.
- Be aware that someone who has remote access to your computer has access to everything. They can see everything you are doing on it; they can also download other types of malicious software.
- To a scammer your personal information is just as valuable as your money and they will use it in any way they can.
- If you suspect this has happened to you turn off your computer and do not turn it back on, immediately take it to a reputable computer technician.
- Contact your bank to report what has happened so they can help to protect your financial accounts.

*Remember never disclose your security codes, like your Westpac Protect SMS code for online banking, to anyone. This is how we keep you safe and know it is you completing the transaction. It is ok to hang up and seek help, by contacting Westpac on **132 032**.*



Protect yourself from scammers.

- Is the request genuine? Research who you are dealing with, or get a trusted second opinion.
- Keep security software up to date on all devices. Do not open suspicious texts, pop-up windows or emails – delete them.
- Keep your personal/business details secure.
- Do not share passwords and security access codes.
- Use unique passwords for all online accounts and change frequently.
- Beware of requests for your details and or money; this includes unusual payments and deposits.
- Be open with the bank regarding your transactions. The bank needs all the information to protect your money.
- Regularly visit your banks' security page and **www.scamwatch.gov.au**

Fraud.

Fraud happens when transactions occur on your accounts without your authorisation.

Online retailers and payment service providers are doing more than ever to adjust their frameworks in order to reduce fraud numbers in Australia.



In 2018, despite reporting a decrease in overall fraud cases, there was still

4.35 million

reported fraud transactions on Australian-issued cards.



Australian-issued card fraud cases resulted in a value of

\$574 million in losses.





Common types of fraud.

Card fraud

Card fraud is where your credit, debit or handycard is used by one of the following methods:

- Card is compromised by a skimming device which could be attached to an ATM or EFTPOS terminal
- A data breach at a merchant
- Your card is lost or stolen
- Your identity is compromised and used to order a new card

Fraud can then be committed using online card payments, your card details copied onto another card (counterfeit) or using your stolen card to make purchases you are unaware of and have not authorised.

Cheque and Transaction fraud

There are different types of cheque and transaction fraud:

- Altered cheques
- Counterfeit cheques
- Stolen cheques
- Money taken without your authorisation
- ID fraud
- Signature fraud

Identity fraud

Identity fraud is a type of fraud that involves the theft of your personal information, including your name, date of birth, address, and other details. It can be used to steal money or gain other benefits. There are several ways it can occur. It starts with stealing your private information through the compromise or theft of your physical documents. Or the use of fraudulent text messages and emails asking you to provide personal data.

Once your identity is compromised it could be used to:

- Withdraw money from your account
- Open accounts and services in your name
- Obtain loans in your name



Eleanor's story of ID fraud.

Eleanor went into the branch, as she had not received her bank statement. In fact, she had not received a number of expected bills either. Upon chatting to the staff, she learned her statement had been sent two weeks ago and she should have received it by now.

The bank staff noticed that Eleanor had made a number of account enquiries recently, some maintenance, as well as a personal loan application. All of which, Eleanor explained, she had not completed.

The bank placed a stop on the application and secured Eleanor's accounts. She was instructed to contact ID Care to take further precautions to protect her identity. It was later learned that mail had been stolen from a number of residences in the same group of units.

The perpetrator, a caretaker of the facility, had access to their mailboxes. The caretaker was able to obtain personal information required to pretend to be Eleanor or one of her neighbours.

Protect yourself from fraud.

To prevent yourself from falling victim to fraud there are a number of steps and checks you can put in place, and regularly monitor to maintain your safety and privacy, such as:

- Protect your privacy on social media.
- Ensure your mailbox is locked.
- Safely dispose of personal and financial information.
- Sign up to electronic statements.
- Check you've received all expected bills and statements.
- Ensure all of your contact details are up to date with the bank including email, address and phone numbers.
- Contact the bank about ways to increase your security either by adding verbal passwords or registering for SMS protect.
- Check any cheques you receive for inconsistencies and report missing/stolen cheques/cheque books to us immediately.
- Place a hold on or report your card if you believe it has been lost or stolen.
- Never share/disclose pin numbers to anyone.
- Never keep your banking codes and password together.
- Check all bank statements and report suspect transactions.
- Regularly check or set up alerts for when someone accesses your credit file and report any discrepancies.



We can help.

We understand that it can be hard to talk about, or take action to stop financial abuse. In our branches, you can speak with one of our staff members separately from your support person, friend or carer.

When you tell us that you suspect financial abuse, depending on your personal circumstances, we may:

- Put activity on your accounts on hold or delay specific transactions while we investigate your situation.
- Check that any person acting on your behalf has the appropriate authorisation based on the information available to us.
- Help you to understand your existing financial arrangements with us.
- Help you change any online banking login details and PINs to better protect your money and the security of your information.
- Help you change the address for mail that we send to you, including any new cards. You may wish to nominate the address of a trusted person, or your local branch.

If you think you have been impacted by financial abuse, a scam or fraud, **contact Westpac immediately.**

 **132 032**

Additional help.

IDCARE provides free, confidential support and guidance to people who have been targeted by fraud, scams, identity theft or compromise.

If you think your personal information or financial security may have been compromised, you can contact IDCARE toll-free on **1300 432 273**, or visit their website **www.idcare.org**

Lifeline provides Australians experiencing a personal crisis with 24 hour crisis support and suicide prevention services. Lifeline can be contacted on **13 11 14**.

For any additional help and support you can get in touch with:

- Your bank or credit union
- Trusted family or friend
- Local police

Report all scams to:

- cyber.gov.au/report
- Westpac.com.au/security
- idcare.org
- staysmartonline.gov.au
- scamwatch.gov.au

Other help numbers.

ACT

Elder Persons Abuse Prevention Referral and Information Line (APRIL)

02 6205 3535

ACT Disability, Aged and Carer Advocacy Service (ADACAS)

02 6242 5060

NT

Elder Abuse Information Line

1800 037 072

NSW

Elder Abuse Helpline

1800 628 221

QLD

Elder Abuse Prevention Unit

1300 651 192

07 3867 2525 (Interstate)

SA

Aged Rights Advocacy Service

08 8232 5377

Elder Abuse Phone line

1800 372 310

TAS

Tasmanian Elder Abuse Helpline

1800 441 169

or

03 6237 0047

VIC

Senior Rights Victoria

1300 368 821

Elder Rights Advocacy

03 9602 3066

or

1800 700 600

WA

Elder Abuse Helpline

1300 724 679

Advocare

1300 724 679 (Perth)

1800 655 566 (Rural)

Any questions?

Anyone can fall victim to financial abuse, and unfortunately, it's not always as obvious or traceable as we would like.

By checking your accounts and communications on a regular basis, keeping personal information private, and seeking assistance from trusted sources, the chances of financial abuse happening to you can be significantly reduced.

However, due to the nature of scams, fraud, and manipulation noticing when something isn't quite how it should be is not always immediate. We understand this and will always make time to assist with any worries or suspicions you may have about your financial security - or steer you in the right direction for the kind of help and support you may need.

Perhaps something you've read in this brochure has set off alarm bells for you. Maybe it has just left you feeling a little uneasy. No matter how big or small, if there's something worrying on your mind that we haven't covered - don't hesitate to get in touch.



Glossary.

Term	Definition
Fraud	A Fraud is when the customer did not authorise the transaction and/or method of loss. An example of fraud could be that your credit card is lost or stolen and then used by the fraudster.
Scam	A Scam is when the customer willingly participated in the transaction but has been misled regarding the benefit or purpose. They can be more challenging to detect as they are disguised as genuine transactions.
Financial abuse	Financial abuse occurs when someone manipulates your financial decision-making, or misuses or controls your money, financial resources, or property or assets without your knowledge or consent.
Power of Attorney	A Power of Attorney is a formal instruction whereby a person (who is called the Donor) appoints another person (called the Attorney) to act on their behalf. Power of Attorney ends with the death of the Donor or the loss of mental capacity of the Donor.
Enduring Power of Attorney	An enduring power of attorney is a legal document which you can use to appoint a person to make decisions about your property or financial affairs which continues even after you have lost mental capacity..
Vested interest	A personal reason for involvement in an undertaking or situation, especially an expectation of financial or other gain.

Term	Definition
Guarantor	Person giving a guarantee and who assumes liability.
Will	A Will is a legal document that contains information on who receives assets and belongings after a death. A Will can also be used to appoint a guardian to look after children until they are old enough to look after themselves.
ACCC	Australian Competition and Consumer Commission; the statutory authority that administers the Trade Practices Act 1974 and the Prices Surveillance Act 1983, and has additional responsibilities under other legislation on competition matters and consumer protection.
Remote access	Remote access is a form of software which allows a Scammer to take full control of your computer, viewing all your screens including your browser when you sign into Online Banking.
Social media	Websites and applications that enable users to create and share content or to participate in social networking.
IDCARE	IDCARE is Australia and New Zealand's national identity and cyber support service.

We're here to help.

 132 032

 [westpac.com.au](https://www.westpac.com.au)

 Visit us in branch

