Protecting yourself and your loved ones from elder financial abuse

Colonial First State

Contents

The real impacts of elder financial abuse

Financial abuse can take many forms, from scams and fraud to emotional blackmail and theft, and it can be committed by strangers, friends or even family members. Elderly people are particularly vulnerable to this kind of mistreatment and the impacts can extend beyond financial loss – for example, causing anxiety and depression, or preventing access to food, medical care and safety.

That's why it's so important for us to work together as a community to keep everyone safe from elder financial abuse. If an elderly friend or relative is alone or isolated, has a physical or mental disability, is reliant on others for their care, experiences language difficulties or has a limited understanding of finance, then they are especially at risk of experiencing elder financial abuse. And of course, these are all risk factors for you as well.

Older people tend to be less tech-savvy than their younger counterparts, and this makes them more likely to fall victim to online scams or fraud. It's hard to assess the scope of the problem because a lot of people don't realise they've been the victim of a scam or fraud. And those who are aware may feel ashamed to admit it or report it.

We do know, however, that the real impact of fraud and scams is a great deal higher than most people imagine:

176m	**There was more than $176 million in lost funds reported to Scamwatch in 2020[1]**
41%	**41% of the losses were for people aged 55 and over[1]**
23%	**Reported losses increased by 23% between 2019 and 2020[1]**

Spotting elder financial abuse

Elder financial abuse can take many forms. It could be repeated incidents or one-offs, threats or even a lack of action. Here are 10 of the most common types of abuse.

Abusing power of attorney	Pressure, threats and intimidation	Fraud and scams	Abusing family agreements	Improper use of funds
Abuse can happen when a trusted person is given power of attorney over someone's assets, and they abuse their ability to make decisions for them.	This could be physical or emotional pressure on an older person to make them a beneficiary of their Will, or sign over ownership of assets.	This is when a third party sets out to falsely gain a person's trust to defraud them and steal their money.	Families sometimes enter into informal agreements designed to help everyone, but this can unintentionally create opportunities for abuse.	This is when someone lawfully has access to an older person's money, but they use it for purposes they had not agreed on.
Theft	**Inheritance impatience**	**Guarantors gone wrong**	**Failure to provide promised care**	**Emotional blackmail**
Older people are particularly at risk of theft, especially if they have care needs. Thieves can exploit anyone's physical or mental vulnerabilities.	Sometimes people feel entitled to an ageing relative's assets and so they access them, even while their relative still needs them.	Well-meaning older parents sometimes act as guarantors to a child's home or business loan, but they could lose their home if the loan is in arrears.	A change in circumstance (like employment) can cause the breakdown of a financial arrangement to look after an ageing relative.	This is one of the least visible forms of abuse and can occur when an emotionally-dependent adult child abuses their parents' concern by demanding money.

Common features of all types of elder financial abuse

There are four main features common to all types of elder financial abuse:

1

Financial abuse exploits a power imbalance

When a person reaches their elder years, they usually experience a reduction in their mental and physical capacities. A younger, more able-bodied person can take advantage of this to intimidate the older person, especially if the older person is reliant on them for care.

2

It’s an abuse of trust

Often elder financial abuse occurs where there is an expectation of trust. This could occur in a pre-existing relationship (e.g. family), or in a new relationship that may appear genuine, but has really been created out of self-interest.

3

It’s often not technically illegal

It can involve someone unethically exploiting their Power of Attorney or other legal mechanisms that give them control over an elderly person’s assets.

4

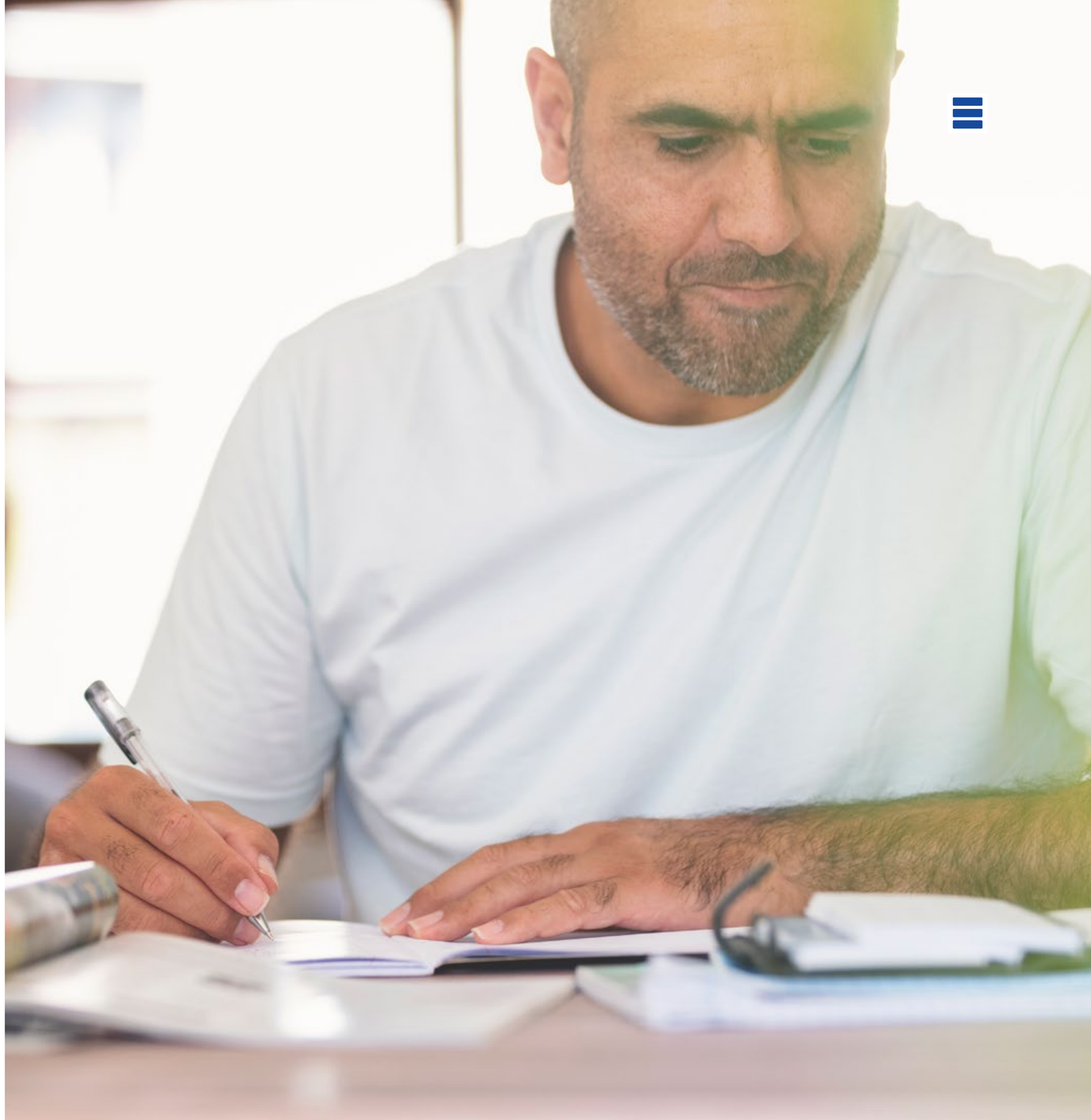
It often causes psychological, not physical harm

Elder financial abuse doesn’t usually involve obvious physical threats or violence. Instead, the abuser inflicts profound emotional harm and psychological distress on the victim.

Fraud and scams

With more of our lives moving into the digital world, scams and fraud are becoming increasingly common. Fraud usually happens when somebody accesses your money without your knowledge or authority. You might not even be aware of the fraud until you notice it on your statement or receive a call from your bank. A scam happens when somebody gains your confidence in order to steal your money or information.

Scammers often use sophisticated lies to trick people. By recognise the warning signs for common scams and types of fraud, you can avoid losing your money to someone who is trying to take advantage of you.



Common scams

- **IT support** that requires access to your computer via installed software
- **Romance and dating scams** where the scammer forms a relationship with you to extract money or gifts
- **Investment scams** where the scammer offers fast, high returns
- **Job opportunities** with promises of fast, fool-proof money for little effort, like multi-level marketing or pyramid schemes
- **Unexpected money** offered through a lottery or Nigerian scam where you pay a small amount upfront for a larger share later
- **Travel scams** offer fake free or discount holidays and ask for credit card or bank details
- **Fake charity** scammers prey on your compassion to get bank details for one-off or ongoing donations
- **Buying or selling products** that either don’t exist or don’t work as described

Common types of fraud

- **‘Phishing’** is where you are tricked into providing login or credit card details via a suspicious phone call or a link to a fake website
- **Malware** installs software on your computer after you click on a link in a legitimate looking-email, giving criminals access to your bank accounts
- **Skimming** happens when a device is installed on an ATM or EFTPOS machine that stores information from cards to use fraudulently later
- **Card fraud** is when your credit card details are used without your authorisation
- **Missed call** from unknown numbers that have a high call charge when you return the call
- **Identity fraud** occurs when your identity or personal information is used to commit a crime, often through false financial documents
- **Cheque fraud** uses fake, forged or altered cheques to pay for goods and services

Real-life scam stories

Here are two stories that bring the reality of scams into focus. These are based on real-life situations that happened to Commonwealth Bank customers.

Neither customer had spoken to anyone about these big financial transactions, but the damage could have been prevented if they had known they could check with the bank or their financial adviser.

Eddie’s story: A romance scam

Eddie, a successful 52-year-old business executive, was widowed and lonely. He met Kali, a beautiful 40-year-old woman of African descent, via an internet dating site. Kali had recently moved from Australia to the United States when her father had died, so she could support her unwell mother. Kali asked Eddie for $933 to pay for some medical tests for her mother. She assured Eddie she would inherit $1 million when her father’s estate was settled. Suddenly, her mother needed an operation that would cost $54,000, and she implored Eddie to lend her the money – which he did.

Before long, he’d loaned her another $492,000 to pay for her mother’s ongoing chemotherapy treatments. Eddie waited patiently for Kali’s call and was shocked when, a week later, he called and the number was disconnected. He realised he had been scammed and had given away $546,933. He approached the bank to see what could be done. The bank immediately froze Eddie’s account and blacklisted the recipients. Unfortunately, the bank was unable to recover the funds because too much time had passed.

Susy’s story: A remote access scam

62-year-old Susy had a large inheritance in an account. She knew about scams and hackers. So, when ‘Tim’ called, saying he was from the security department of her telephone company, she was open to what he had to say. Tim said he had detected a hacker and recommended she buy hacker protection that cost $9,700, and insurance for $8,000. It seemed a lot to Susy, but she knew she had more to lose if she didn’t act quickly.

Tim offered Susy shares in the insurance company he had bought a year ago, and said Susy could buy them in incremental amounts. She wanted to go on holiday, and so she set up an online NetBank account so Tim could make the incremental purchases on her behalf. Tim made transfers that created a flag in CommBank’s system and triggered a lock on Susy’s account. During a visit to the bank, Susy realised her account was almost empty. She admitted to the teller that she had given Tim access to her account. Of the $90,000 Susy had lost, the bank was only able to retrieve the initial transfer of $9,700 made to another financial institution. All of the money ‘Tim’ had transferred from Susy’s account had disappeared.

Real-life stories of financial abuse from friends or family members

Scams are common, but so are cases of financial abuse by friends or family members. These stories are based on real-life situations that happened to Commonwealth Bank customers.

Brian's story: Money disappearing from bank account

70-year-old Brian was struggling with health issues, so his son Wayne did his shopping for him. Wayne set his dad up with an online account and helped him pay his bills. Without his father's knowledge, Wayne started to use his dad's account to pay for small bills when money was tight. He intended to pay the money back later, but never seemed to have enough money to do so. Brian continued to receive his bank statements by post. He noticed some transactions he didn't recognise, and so he called his bank.

The bank investigated and was able to identify these amounts as being spent on Wayne's utilities and shopping accounts. Brian questioned Wayne about the transactions, and Wayne was very apologetic and embarrassed. Brian acted on the advice of his bank and sat down with staff to discuss a safer way of handling his banking needs, such as setting up autopay on regular bills.

Maddy's story: A very uncomfortable conversation stopped her from losing everything

Maddy, a 65-year-old woman, accompanied her young next-door neighbour, Kay, to the bank. Kay was getting divorced and needed $260,000 to buy out her ex-husband so she could remain living in their family home. Maddy wanted to loan Kay the money, and Kay had promised to pay it back with an inheritance from her very elderly father soon.

The bank teller was worried. There weren't any legal documents for the loan, and it didn't seem like Maddy had sought advice from anyone. After talking with the bank manager, the bank teller suggested putting the transaction on hold for 24 hours until Maddy discussed the loan with family members, an accountant or a solicitor. Maddy was upset and embarrassed by the teller's request, but reluctantly agreed. Kay angrily demanded that the bank honour the transaction but, as she had no formal authority over the account (such as a Power of Attorney), the transaction was put on hold.

A few days later, the branch manager called Maddy to follow up. Maddy said that after discussing it with her family, she realised what could have gone wrong and was grateful that the bank had saved her from potentially losing all her savings.

What to look for

When making decisions about your money, you may not be aware of some of the risks you face. Here are some of the things to look out for:

Incredible offers to make easy money

If it sounds too good to be true, it almost certainly is! Be particularly cautious if these offers come from strangers.

Unknown contact

Be wary of accepting unexpected phone calls, emails or requests for remote access to your computer or accounts – even from your friends, family or third parties you believe you can trust. If you think a phone call sounds suspicious, hang up. Don't click on links or open email attachments unless you know what they are.

Seeming bullied or rushed

If you're contacted by someone saying they are from a big and legitimate organisation (such as a bank, telephone company, utility company or government department) and that person tries to rush you into something, it probably isn't genuine. If in doubt, you should hang up and call the company directly (after sourcing the number yourself).

Unknown transactions

Keep an eye out for unusual and unknown transactions on your bank statements, whether small or large, particularly for $1 (these small amounts are used to test if an account is active before taking out larger sums of money).

Feelings of intimidation

Feeling intimidated may be a sign that someone is using power to force you to hand over control of your finances. Also, be careful if someone else is asking to withdraw on your bank account or fill out a form for you – unless you know and trust them completely.

How to notice warning signs in others

The best defence against financial abuse and harm is education, awareness and vigilance. Your elderly neighbours, friends and relatives rely on the people around them to protect them from financial abuse – and you may be one of the few people they have to support them. That's why it's so important to be aware of the warning signs in your loved ones that may indicate they are a victim of financial abuse. Here's what to look out for:

Changes

They make a sudden change to the way they do their banking.

This could include:

- withdrawing money more often than usual, or in larger amounts
- transferring a large sum of money overseas
- giving someone authority to access their account.

Confusion

They seem surprised or confused.

They may have:

- withdrawals from their account that don't make sense
- language barriers that make it hard for them to understand what is going on
- missing or confusing bank statements.

Coercion

They seem to be under uncomfortable pressure to make a decision about money.

Listen to them to understand whether:

- they're feeling intimidated or controlled by someone
- someone has accompanied them to the bank to make a withdrawal
- they allowed someone else to complete documents or forms on their behalf.

Preparation is the best defence

There are certain things you can do to minimise the risk of financial abuse. The more prepared you are, the better equipped you'll be for the future. Here are some steps you can take right now.

Protect your passwords

It's important to keep your passwords, PIN numbers and personal information secure at all times – so never share these, even with someone you know. Try to use words and numbers that can't easily be guessed – and don't use the same password for everything. You should also avoid writing these down or storing them somewhere obvious (like your wallet).

Stay safe online

Make sure your computer is protected with up-to-date virus software. Always use secure websites when shopping online, and don't send money or personal information to people from unusual locations. When making purchases in stores, avoid swiping your card – insert or tap it instead. Check your bank account and statements regularly to watch out for unusual activity.

Take security measures

Banks have ways to protect their customers' assets – like allowing you to set up others with access to their bank account (but not loans or credit cards) without giving them full Power of Attorney rights. Speak to your bank about putting controls in place to lock or block certain types of payments, put a cap on your spending, or set limits on transactions.

What to do if you’re a victim

If you or a loved one does fall victim to a scam or fraud, it’s best to take action straight away. You can:

Let your bank know

Contact the bank immediately if you notice any unusual or suspicious transactions. You should also tell bank staff if you need an interpreter or have any hearing or other impediments.

Change your passwords and PINs

Make sure you change the passwords and PINs on all your accounts and cards, not just the ones you think are affected.

Report the scam

Call IDCARE – a free, government-funded service – on 1300 432 273. You should also report scams to the relevant government agency.

Get government assistance

If you’re a victim of identity crime, you can apply for a Commonwealth Victims’ Certificate. If you’re feeling scared, contact the police or seek advice from an Elder Abuse or Seniors Rights Helpline.

Choosing the right support network

Everyone wants to be independent, especially as they get older. But it’s essential to gather a trusted support team around you that you can rely on to help if (and when) the need arises. Your support team could include family members, doctors, bank staff and your accountant, lawyer and financial adviser.

Everyone has a role to play

Doctors

- Assess health through regular check ups
- Determine your capacity to manage your financial affairs
- Help decide when a Power of Attorney takes over

Lawyers and community legal centres

- Help draft your Will and create a Power of Attorney
- Formalise family agreements
- Prevent financial abuse or unintentional harm

Accountants

- Help with tax, business and property arrangements
- Keep track of your everyday spending
- Detect unusual or suspicious transactions

Financial advisers

- Help with retirement planning
- Tailor investments to match your appetite for risk
- Structure personal and business finances

Bank staff

- Assist in managing everyday finances
- Arrange an ‘authority to operate’ on your accounts
- Investigate any suspicious transactions

Family members or carers

- Help with financial, legal and health-related matters
- Assist with your health, safety and emotional wellbeing
- Help you understand your options and advise you on decisions

What is Power of Attorney?

A Power of Attorney is a legal document that allows you to appoint someone to make decisions about property or financial matters for you. The main factor determining when someone uses this authority is a decline in your mental health. But there are other reasons you might need a Power of Attorney – for example, if you're injured, in hospital, living in a remote area or travelling in a foreign country.

General Power of Attorney (GPOA)

GPOA is only effective while you have the capacity to make and communicate decisions for yourself. It allows your Attorney to act for you in financial and legal matters – such as managing property and shares, operating your bank accounts, spending money or making gifts. You choose when and for how long this power lasts – so it can be useful if you need someone to act on your behalf for a specific period of time.

Enduring Power of Attorney (EPOA)

EPOA allows your Attorney to make financial decisions on your behalf if your capacity to make decisions is lost or diminished. You can set limits and decide when it comes into effect. Choosing your EPOA is an important decision about what happens to your financial affairs if your health deteriorates. Because the role has significant authority, it's best to choose carefully – and speak to a financial adviser about how to protect yourself.

Choosing your Power of Attorney

The person or people you choose to appoint with 'Power of Attorney' will play a major role in the future of your financial and legal affairs – so it's important to select someone with financial sense and knowledge who you trust to stand up for your rights. Remember, this does not have to be a family member. A lawyer or State Trustee can help you set this up to ensure you follow correct processes.

It's important to start thinking about your Power of Attorney while you're in good health and have plenty of time to prepare. You should be specific and detailed about the powers you're assigning to your Attorney. To reduce risk, consider granting authority for a fixed period of time only, assigning authority to multiple people, or setting limits on transactions. You also need to review your Power of Attorney regularly – and if you make changes, tell your bank and anyone else who has a copy as soon as possible.

Where to get support

Fortunately, there are plenty of resources and support services available for elderly Australians, ranging from advocacy and advice to assistance with money management and accessing benefits. These include:

National resources

Providing information, support and mediation

Aged Care Complaints Commission
www.agedcarecomplaints.gov.au
Ph 1800 550 552

Respecting Elders – FMC Mediation & Counselling
www.mediation.com.au
Ph 1800 214 117

Relationships Australia
www.relationships.org.au
Ph 1300 364 277

Legal assistance

Providing free legal advice and support

Australian Financial Complains Authority
www.afca.org.au
1800 931 678

IDCARE
www.idcare.org
Ph 1300 432 273

National Association of Community Legal Centres
www.naclc.org.au

Senior advocacy

Making sure your voice is heard

Aged and Disability Advocacy Australia
www.adaaustralia.com.au
Ph 1800 818 338

Council on the Ageing
www.cota.org.au
Ph 02 6154 9740

National Seniors Australia
www.capacityaustralia.org.au
Ph 0400 319 089

Aged care information

Providing financial and legal information

Senior Rights Services
www.seniorsrightsservice.org.au
Ph 1800 424 079

My Aged Care
www.myagedcare.gov.au
Ph 1800 200 422

National Aged Care Advocacy Helpline
Ph 1800 700 600

Money management

Tools and resources for planning your financial future

ASIC MoneySmart
www.moneysmart.gov.au

National Debt Helpline
www.ndh.org.au
Ph 1800 007 007

No Interest Loan Scheme
www.nils.com.au
Ph 13 64 57

Centrelink advice

Contacting the Department of Human Services

Pension Payments
www.humanservices.gov.au
Ph 132 300

Carer Payment
www.humanservices.gov.au
Ph 132 717

Special Benefit
www.humanservices.gov.au
Ph 132 850

Want more information?

If you'd like more information about how to protect yourself or a loved one from financial abuse, talk to your financial adviser or call us on 13 13 36, Monday to Friday, 8am to 7pm, Sydney time.

1 Australian Competition and Consumer Commission, *Targeting scams 2019*, 22 June 2020

28446/FS7596/0522