# Submission

| | |
|---|---|
| **To** | Parliamentary Joint Committee on Corporations and Financial Services |
| **Topic** | Inquiry into financial services regulatory framework in relation to financial abuse |
| **Date** | 13 June 2024 |

**Contact**

**E** advocacy@unitingcommunities.org

**P** 08 8202 5111

UNITING COMMUNITIES

# About

We are an inclusive not-for-profit organisation working alongside more than 80,000 South Australians each year and have been creating positive change for South Australian communities for more than 120 years. We advocate for systems change across diverse social justice issues to shape public and social policy that delivers better outcomes for marginalised communities.

We support those in need to find the courage to move forward through enriching their lives and uniting the communities in which they live. By tackling the deep-seated challenges that affect people's lives, we are working to create systemic change and brighter futures for all South Australians.

We provide support services across a range of different areas including legal services, aged care, family and domestic violence counselling, alcohol and other drugs, disability, homelessness, mental health, and child protection.

We understand that dealing with the legal system can be confusing and daunting and staff in the Uniting Communities Law Centre assist people to work through these challenges. The qualified team provides support with information, advice, representation, referrals, or community legal education and in most instances these services are free.

Our Law Centre also includes a specialised Elder Abuse Unit which provides legal and social work support to people over the age of 65 impacted by elder abuse. Our focus is always the older person. We start by speaking with them and getting their permission to make an appointment. We then do a broader assessment to work out what's going on and develop a way forward. Support can include legal representation, case management and counselling.

The Law Centre also has a Consumer Credit specialist service that works alongside the Elder Abuse Unit and has assisted with claims against banks, financial services and/or credit providers in cases of elder abuse.

We are also a provider of the Escaping Violence Payment (EVP) which is available to anyone over 18 years old, who has recently experienced intimate partner violence, has changed living situation and is experiencing financial stress. Eligible clients can receive up to $5,000 in financial assistance.

# Submission to the Australian Parliamentary Joint Committee on Corporations and Financial Services inquiry into financial services regulatory framework in relation to financial abuse

Uniting Communities thanks the Parliamentary Joint Committee on Corporations and Financial Services for undertaking an inquiry into financial services regulatory framework in relation to financial abuse.

Financial abuse impacts a variety of people including those experiencing family and domestic violence and elder abuse. Importantly, financial abuse is not limited to relatives or intimate partners but can also be perpetrated by relatives who are not in an intimate partner relationship such as children towards parents and non-relatives such as aged care workers or informal support workers as well.

We work directly with individuals and families that have been impacted by financial abuse and understand the challenges and obstacles experienced by victims when seeking support from banks and other financial services. Our submission strongly focuses on the impact of financial abuse on older people, given our expertise within our Law Centre (including the specialist Elder Abuse Unit), and because we believe this cohort is increasingly vulnerable to financial abuse due to the rapid changes of digital technology.

## Our key recommendations:

- **Policy and reform on financial abuse must not be limited to victims of intimate partner violence but must consider other vulnerable cohorts as well such as older people.**
- **A legislative obligation should be implemented that requires banks to detect and notify customers when there is a change in spending patterns (suspicious activity detected that could be indicative of financial abuse) in accounts and make active efforts to resolve the issue with the customer.**
- **Banks have a legislative obligation to invest and utilise suspicious activity monitoring technology to detect and monitor for changes to transaction patterns that may be indicative of financial abuse.**
- **Banks have a legislative obligation to conduct an assessment with customers before transitioning them to online banking. Similar to responsible lending laws which require the lender to assess that a proposed credit contract is not unsuitable, a similar duty should also apply to transitioning customers to online banking.**
- **Banks provide an agreement/form for situations where customers need to share their password/PIN code with another person to support them in paying bills online. The signatory must not use their access for any transactions other than what was originally intended. Appropriate penalties for any misuse of access should be instituted and any potential signatory informed of the penalties prior to becoming a signatory.**
- **Banks should be given exemptions against the *Privacy Act 1988,* when matters involve suspected financial abuse, in circumstances where a specialist elder abuse unit contacts the financial institution seeking to immediately freeze/block access to accounts from suspected perpetrators so that the bank can act quickly as a matter of urgency.**
- **Banks should have exemptions against discrimination claims through the *Age Discrimination Act 2004* and/or *Disability Discrimination Act 1992* where there are reasonable grounds to suspect financial elder abuse so financial institutions can better protect older customers.**

- **The commitment to provide inclusive and accessible banking services to older customers under chapter 13 of the Banking Code of Practice be adopted into a legislative duty. Banks must be required to provide alternative solutions and support to customers who inform them that they are unable to access/use online/digital banking products.**
- **Both banks and the federal government provide digital literacy and financial literacy training options for people, particularly in regional areas, so that customers are not put in a position where they are forced to rely on others to access their banking through digital channels. Digital literacy and financial literacy training options need to include face-to-face delivery.**
- **Banks implement mandatory training for customer service staff, so they are well versed in how to identify financial abuse and how to respond appropriately and sensitively to older customers who prefer not to use digital banking.**
- **Third-party signatories are required to sign a declaration that they will not misuse the arrangement for their own benefit (with the Justice of the Peace or staff as a witness). Customers must be provided with appropriate education on the power of third-party signatories to their accounts before approving a third-party signatory. Appropriate penalties for any misuse of access should be instituted and any potential signatory informed of the penalties prior to becoming a signatory.**
- **Banks provide better education through public awareness campaigns to the public and older customers about the variety of options available with account management such as opting into protective management measures such as:**
  - **'two to sign',**
  - **pre-set limits,**
  - **getting transaction notifications,**
  - **using dedicated cards and PINs for those authorised to access their banking and**
  - **limiting the type and amounts of transactions.**
- **That every bank has a Vulnerable Persons Unit to support victims of financial abuse and those at risk of financial abuse.**
- **The government lead early intervention and prevention strategies by increasing awareness of financial abuse and providing adequate funding for support services that assist victims of financial abuse.**

## Additional Comments

### 1. The prevalence and impact of financial abuse of older people

We acknowledge that anyone can be impacted by financial abuse, and that it is not limited to family relationships or intimate partners. However, we know that women experiencing domestic and family violence, culturally and linguistically diverse people, people living with disability and older people are disproportionately at risk.

For example, due to rapid changes in technology, some older people may not have the digital literary skills to conduct online banking and may have to rely on others (who may perpetrate financial abuse) to do this for them. They may also not monitor their online accounts regularly preferring to wait for the paper bank statement to arrive, leaving them vulnerable to financial abuse in the meantime. The closure of physical bank branches is limiting access for some older Australians that rely on over-the-counter transactions to enable them to retain control of their banking.

Uniting Communities has been collaborating with Flinders University on a research project utilising the data and expertise of our specialist Elder Abuse Unit. The resulting data found that out of 724 referrals to our Elder Abuse Unit, 54.4% involve financial abuse (which increases to 62% for women) and 63% of perpetrators are adult children of the victim. Financial losses arising from financial abuse include small amounts taken over a long period of time and cases where large amounts of money are stolen. A common issue with financial abuse reported by the Elder Abuse Unit involves unauthorised transactions to a person's transaction account performed electronically. There have been instances where perpetrators have used debit cards, internet banking or mobile phone apps to make purchases or withdraw money without the consent of the person impacted by financial abuse. When it comes to risks for financial abuse, older people are a particularly vulnerable cohort of the population.

The impact of financial abuse cannot be overstated. It can have life changing consequences by impacting the victim's housing situation, health, wellbeing, and autonomy. For older people who do not have the capacity to regain the financial losses from the perpetrator and/or work to acquire more income, it is particularly devastating. Older people can lose a lifetime of wealth and savings and are unable to financially recover. This has compounding effects if they have lost their savings, it then becomes an issue for the government to entirely fund social security and aged care support as a result.

### a. The approaches taken by banks to identify, record and report financial abuse, and any inconsistencies arising therein

The current approaches by banks to detect and respond effectively to financial abuse are inadequate. Our experience is that banks often fail to detect uncharacteristic transaction activities that are indicative of financial abuse. It can take the bank a long time to realise transactions are suspicious, at which point the victim may have sustained a significant financial loss. Often these are not technical nor vague differences in spending but are obvious and could have been easily detected with current suspicious activity monitoring technologies.

For example, an elderly person "appears" to suddenly access online shopping and gaming websites when they have never previously done so. Or where an account holder who is resident of a residential aged care facility suddenly has transactions for cigarettes and alcohol located in night clubs in the early hours of the morning. In addition, even when banks are informed directly by the customer that financial abuse has occurred, banks sometimes do not respond quickly enough.

Software and detection technology/tools could be implemented to monitor abnormal spending habits. Banks have access to such technology, especially with the advancement of AI algorithms. Investment in this technological infrastructure is vital to protecting customers. Suspicious activity monitoring technology that is currently being used by banks to monitor fraud and scams should also, by legislative requirement, be used to detect uncharacteristic behaviour that could be indicative of financial abuse. This should be a legislative duty rather than the current self-regulation through section 4.3 of the ABA Industry Guidelines, which is not legally binding and not sufficiently protecting older customers from financial abuse.

Banks are already subject to a duty under Anti-money laundering and Counter Terrorism Finance legislation to submit a 'Suspicious Matter Report' to AUSTRAC if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law and transaction monitoring obligations under this legislation already requires banks to have regard to size, frequency or patterns of transactions that may indicate unusual or suspicious activity, including suspected fraud or identity theft.[1]

[1] Ongoing reporting obligations, 2024, https://www.austrac.gov.au/business/core-guidance/reporting#:~:text=You%20must%20submit%20suspicious%20matter,business%20days%20for%20anything%20else.

Banks do not currently have a legislative obligation owed to customers to monitor, detect and respond to abnormal spending. The banks contractual duty does not extend to monitoring accounts under common law. This was illustrated in the Australian Financial Complaints Authority (AFCA) Determination 831545 April 2022 where the legal principles were summarised as:

> *A banks relationship with their customer is an ordinary commercial one and a banks duty is to follow the customer's mandate or instruction. This means that a bank does not generally have an obligation to:*
> - *monitor a customer's use of funds on their behalf,*
> - *maintain watching briefs for scams,*
> - *prevent the customer from dealing with funds they are contractually entitled to access, and/or*
> - *reimburse a customer for authorised payments to a third-party.*[2]

Additionally, there is no duty in contract or negligence law to monitor accounts. In the South Australian *Politarhis v Westpac Banking Corp* [2009] SASC 96 case, the Full Court of the Supreme Court said in relation to a tortious duty of care a credit union owed a customer whose employee used its account for gambling:

*'It would be unrealistic to conclude the [bank] was under a duty to monitor and analyse the manner of use by each of its members of their accounts to exercise a form of paternal concern when it saw transactions which were unusually large or unusually frequent.'*[3]

Often customers are led into a false sense of security by advertisements from financial institutions about fraud detection into believing that their accounts are secure and protected from unauthorised transactions involving financial elder abuse. Many customers will report that they expected the same monitoring that previously applied to suspicious credit card transactions to equally apply to current transactions with their bank accounts. Customers who rely on misleading and deceptive conduct provisions in the Australian Consumer Law to claim compensation, often struggle to establish that their loss was causally linked to the conduct of the bank or credit union advertisement as to surveillance and fraud detection.

**Banking Code of Practice - 'Vulnerable'**

It is not compulsory to be a member of the Australian Banking Association and/or subscribe to the Banking Code of Practice. However, there are current provisions in the Banking Code of Practice whereby if a customer who identifies themselves as vulnerable to the bank, the bank needs to 'take extra care' when dealing with the customer. However, 'taking extra care with customers who are experiencing vulnerability,' does not specifically include an obligation to monitor uncharacteristic or unusual patterns in transaction activities. Furthermore, the duty to take extra care is limited to only when the customer tells their bank about their vulnerable circumstances. Our experience working with victims of financial elder abuse is that the duty to take extra care, is ineffective as it relies on customers to first identify themselves as vulnerable. People are often reluctant to identify themselves in this way and/or they do not even realise they would be considered vulnerable by their bank. The duty to exercise 'extra care' is also fraught as ambiguous and it is unclear whether this is meaningless with respect to creating any enforceable contractual obligations. Clients are often coached to identify themselves as vulnerable to their bank and refer the bank to the Banking Code of Practice when asking for assistance on what account features are available to protect against abuse in the future.

---

[2] Australian Financial Complaints Authority, 2022, AFCA Determination Case Number 831545 https://www.afca.org.au/what-to-expect/search-published-decisions, p.2.
[3] Supreme Court of South Australia, 2009, *Politarhis & Anor v Westpac Bank Corporation* [2009] SASC 96 <https://jade.io/article/92802>.

Whereas, in the ABA industry guidelines that exist to complement the ABA Banking Code of Practice (but are guidelines only and do not have legal obligations or prescribe legally binding obligations on subscriber banks), details extra care to include training staff and working with customers to find a suitable way to undertake their banking for when a customer identifies themselves as vulnerable. The ABA Industry Guidelines includes 'bank should be aware of potential warning signs of financial abuse," including when the customer "makes unusual or uncharacteristic transactions."[4] As well as 4.3 advising "banks use software and other digital tools to identify 'suspicious transactions' including fraud." There is a mismatch between the common law which says banks do not generally have an obligation to monitor a customer's use of funds on their behalf, with what the ABA encourages member banks to incorporate into their internal processes, procedures and policies.[5]

**Legislative obligation**

A legislative obligation should be implemented that requires banks to detect and notify customers when there is a change in spending patterns (suspicious activity detected) in their accounts and make active efforts to resolve the issue with the customer. This could be incorporated into new legislation that includes Authorised Deposit Taking Institutes (ADIs) and credit unions as well as banks. This would be an important protection against financial abuse. It could provide a means for victims to seek compensation when their accounts have been mismanaged/exploited by giving the court and AFCA the ability to award compensation where a bank has failed to monitor and intervene appropriately. This would require banks to utilise technologies and update internal policies and procedures to ensure customers are being protected from financial abuse.

International example:
The Australian Parliamentary Inquiry into Fraud and Financial Abuse noted that in California, 'legislation has been introduced making it compulsory for banks and financial staff to report any suspected cases of financial abuse. Where a report is made, adult protective services are called in to investigate.' In Canada, older persons have begun 'authorising their bank to monitor their accounts for unusually large transactions or unusual patterns of transactions. The bank is then authorised to raise its concerns with the account holder and to warn them of the possibility of fraud. Account holders, however, retain full rights over their accounts and may elect to disregard any warnings given.'[6]

## b. The impact of the shift of financial products to online platforms

The shift to online and digital banking platforms has created significant challenges, particularly for people living in regional areas, culturally and linguistically diverse people and older people who do not have access to digital technologies or adequate digital literacy skills. They are then forced to rely on others (family members/non-relatives) to access their bank services, inadvertently making them susceptible to financial abuse. Some older people do not monitor their bank accounts regularly on an app or website but instead wait for a paper statement in the mail (long after the misuse of their funds has occurred).

The Banking Code of Practice states that banks are committed to providing banking services that are inclusive of all people including older people inferring that alternative access options would be made

[4] ABA Industry Guideline: Preventing and responding to financial abuse (including elder financial abuse), 3.2 recognising potential financial abuse as accessed at <https://www.ausfinancial institutioning.org.au/wp-content/uploads/2021/03/ABA-Financial-Abuse-Industry-Guideline.pdf> on 7 June 2024.
[5] ABA Industry Guideline: Preventing and responding to financial abuse (including elder financial abuse), 4.3 Investigate ways to identify potential financial abuse involving digital banking platforms.
[6] Elder Abuse- A National Legal Response, 2017, https://www.alrc.gov.au/publication/elder-abuse-a-national-legal-response-alrc-report-131/9-financial institution/the-reasonable-steps/.

available to online banking. However, our experience is that this is not always the case, even when customers have protested that that they are unable to access online banking and do not want to set up 'computer banking.' Our experience is that customers are coerced into setting up digital banking to access products, such as requirement to refinance loans with a new credit contract or to set up a travel card. This is despite the Banking Code of Practice requiring that banks ensure "bank services are accessible, inclusive and provided to you in a fair and ethical manner."[7] However, by way of example, not all major banks are part of the Australia Post service, Bank@Post, as a face-to-face alternative to over-the-counter transactions where branches have closed.

**Responsible lending laws**

Provisions in responsible lending laws should apply when setting up and establishing an online bank account. Currently, responsible lending laws under the *National Consumer Credit Protection Act 2009* requires that a lender must assess whether a credit contract will be unsuitable for a consumer.

The same should apply to banks when offering online banking services to customers to determine that it is not unsuitable for the customer's digital literacy, creating an obligation for the bank to do an assessment e.g. what are the customer's digital literacy skills and do they have access to the appropriate technology. If online bank access is deemed appropriate staff should go through product features with a customer to explain how they can best protect themselves from financial abuse. This could support the customer to have autonomy and control of their financial assets.

**Sharing of passwords/PIN codes**

Current contractual terms between a bank and customer prohibit customers from sharing their password and/or PIN with any other party. However, this fails to acknowledge that some customers, such as some older people, since branch closures and changes to digital banking, have been given very limited alternatives and are pressured to use online banking without digital literacy or technologies. As a result, they are put in a position where they are forced to depend on others and 'have to' share these details with another person to access their online bank account.

This includes passwords/PIN codes and/or the account is set up using another person's email/phone number. When financial abuse occurs and money has been stolen and misused, it is difficult for the older person to recoup their money back as the bank relies on the contractual terms that the customer breached by sharing passwords, PIN and handing possession of their cards to the perpetrator. The ePayments Code also can produce similar outcomes for unauthorised transactions where the customer is unable to recover losses where they have provided their password/PIN/card out of necessity to a person who has abused their trust.

Cases concerning unauthorised transactions and financial elder abuse, often involve a defence based on the customer willingly providing their pin number/password to the perpetrator to mean the customer is liable for losses where a perpetrator has made unauthorised transactions. However, the Uniting Communities Law Centre is aware of cases where limited authorisation was provided for the purposes of activating an account and/or paying bills, but not for withdrawing money. However, despite the perpetrator lacking authority to withdraw cash, in the vast majority of cases the bank is not liable when the perpetrator has misused these funds without consent from the customer. The general approach seems to be 'all or nothing' that once a person has access to the older person's banking, that there is no protection for

[7] Australian Bank Association, Banking Code of Practice, 2021, <https://www.ausfinancial institutioning.org.au/financial institutioning-code-of-practice-2021-release/>.

transactions which are not authorised. For example, where a debit card is given to an abled bodied family member to purchase groceries and that abled bodied family member uses the card to buy alcohol without the account holder's consent. More can be done by financial institutions to assist older customers with restricting and monitoring access to their accounts to better protect them from abuse.

A written agreement should be created that is signed by the person to whom the customer is giving the authorisation to help with their online banking. The signatory must not use their access for any transactions other than what was originally intended. A Justice of the Peace could be a witness in this process. Penalties should be applied to perpetrators if they fail to abide by the agreement and use the funds for any other purpose other than what was originally intended by the customer. This should be enforced through the criminal justice system rather than civil law processes. Our experience is that sometimes when financial abuse is reported to police, police advise the victim that it is not a criminal matter and a civil matter only. Clearer criminal sanctions would deter financial elder abuse and provide resources for police and courts to pursue and recover financial losses as many victims do not have financial means to pay for a private lawyer.

**2. The effectiveness of existing legislation, common law, and regulatory arrangements that govern the ability of banks to prevent and respond to financial abuse, including the operation of:**

a. **the National Consumer Credit Protection Act 2009;**
b. **the Privacy Act 1988 (Cth);**
c. **the Australian Securities and Investments Commission Act 2001;**
d. **the Insurance Contracts Act 1984;**
e. **legislation and statutory instruments for superannuation; and**
f. **state and territory laws and regulations.**

As mentioned above there is currently no legislative obligation to detect and notify customers when there is a change in their spending patterns (suspicious activity detected) in accounts and make active efforts to resolve the issue with the customer. This includes generally that there is no duty in common law, either in contract or negligence to monitor transactions and act where there are indicators of financial abuse. This presents a significant gap within the laws governing banks as stated above.

**Privacy Act and Age Discrimination Act – carve out protections where elder abuse is suspected**

Currently, there are exemptions within the *Privacy Act 1988* that allow for the disclosure of a person's sensitive personal information without their consent e.g. if is authorised by or under Australian law or court orders, and where disclosure is required to prevent a serious (or in some jurisdictions 'serious and imminent') threat to the life, health or safety of a person and it is unreasonable or impracticable to obtain their consent.[8]

In circumstances where a specialist elder abuse unit contacts the financial institution (after obtaining instructions from the client experiencing elder abuse) in an attempt to urgently prevent further unauthorised withdrawals (except for direct debits for utilities and bills etc.), banks should be exempt from the Privacy Act sanctions. We note that it has not always been possible for the victim to report/or give written authority. For example, an older person who does not have access to technology may not be able

[8] Elder Abuse – A National Legal response, 2017, p. 339

to provide immediate signed written authority. Note this should only apply to freezing accounts and ongoing direct debts for utilities and bills should continue. This exception to the Privacy Act allowing a bank to act on instructions to suspend and block access to banking due to suspected abuse should be limited to reports made by specialist elder abuse units or dedicated police units and should not extend to reports made by the general public as this might open older people up for abuse if this provision is used as a tactic for coercive control.

This would enable banks to act quickly in circumstances of financial elder abuse and given time sensitivities, this can be the difference between losing all the customers' lifetime savings or not. This would also eliminate barriers sometimes experienced by support services when assisting clients experiencing elder abuse. Our service support staff have witnessed some banks do this exceptionally well, which has achieved positive outcomes, and removing these legislative barriers would make it easier for other banks to do this also.

Banks should also have protections against discrimination claims through the *Age Discrimination Act 2004* and/or *Disability Discrimination Act 1992* where they have grounds/reasons to suspect a customer may be a victim of elder abuse. When life savings are involved coupled with a risk for abuse, this would justify a different approach that seeks to protect the customer and their assets. This would give the bank confidence to implement proactive and preventative measures in relation to financial abuse without potential repercussions. Banks currently rely on customers voluntarily notifying the bank that they are 'vulnerable' which doesn't work effectively.

**3. Other potential areas for reform, such as prevention, protection, and proactive systems, including:**

**a. existing financial product design;**
**b. emerging financial products;**
**c. employee training;**

**Access to physical branches and phoneline**

Physical branches are continuing to close across the country. In some regional areas, that have a higher population of older people, this can have devastating impacts when there is no longer a branch available for residents in town. A report by the Senate Rural and Regional Affairs and Transport References committee, highlights that there are significant barriers to accessing digital banking in remote and indigenous communities, particularly for older people.

We strongly support the committee's recommendation that *"the Australian Government adopt a policy recognising access to financial services as an essential service. To this end, it should commit to guaranteeing reasonable access to cash and financial services for all Australians."*[9]

Banks are failing to recognise how important physical branches are to many of their customers including older people or some people living with disability. Quick response times and the ability to speak to a staff member through phonelines (call centres) are also important because for many customers this is pivotal to their access (i.e. phone wait times should not be a deterrent forcing customers to use digital technology and rely on third parties to access their banking requirements).

[9] Rural and Regional Affairs and Transport References Committee, Bank closures in regional Australia, 2024.

Online banking does not and cannot replace physical branches. In complicated cases of financial abuse (for example see case study 3 below) there will always be a need for face-to-face customer service for these difficult matters.

In-person contact is essential to good customer service for many customers and can be a protective measure against financial abuse. If a client attends a physical branch and has direct contact with an employee at the branch who becomes familiar with the customer, the banks employee is better positioned to prevent elder abuse. For example, if the perpetrator of the financial abuse had physically attended the branch to transfer money the employee could have seen the red flags e.g. son accessed the money from their mother's account when they had not done this prior.

Clients of our Elder Abuse Unit have expressed frustration and difficulty when trying to contact banks over the phone and having to explain their situation repeatedly to numerous bank employees instead of speaking with the same staff member that understands their case. In addition, the phoneline itself can be difficult for clients to navigate as they find it difficult to pass the initial automated function e.g. entering their personal customer details before being connected to an operator. Many older customers also experience significant hearing loss making the process increasingly difficult.

Many banks remove their customers' autonomy by making online banking mandatory as it can be inaccessible for some older people. Online banking can also make older people more vulnerable to abuse because it can make them completely reliant on others to operate.

Westpac has made a public commitment not to close any more regional bank branches until at least 2027.[10] In order to fulfill the Bank Code of Conduct that requires services to be accessible, banks must be required to provide alternative solutions and support to customers who inform them that they are unable to access/use online/digital bank products. Banks are taking away their client's autonomy by making online banking mandatory while inaccessible.

**Awareness raising/training for detecting scammers**

Some clients that present to our Law Centre, specifically our specialist Elder Abuse Unit and the Consumer Credit Law Centre, have been victims of online/digital scams. Some older clients are unaware they are involved with a scam until it is too late, such as when Centrelink informs them. This can take time to occur and after which the damage has already been done and recovering the financial loses can be difficult or unattainable.

We believe customers would benefit from more information being shared about the dangers of scammers in paper format (mailing information) and more warnings advertised via a variety of media outlets including, print, radio, television, when customers are navigating their online bank accounts.

**Digital and financial literacy training for customer's particularly older people**

We strongly believe that physical branches should be maintained as a priority so that customers that do not have access to digital technologies can easily retain their access to their bank products. In addition, we believe more digital and financial literacy training, provided by way of face-to-face training, and one-

[10] Bank to keep regional branches open, National Seniors Australia, <https://nationalseniors.com.au/news/latest-news/bank-to-keep-regional-branches-open>.

on-one supports where appropriate, accompanied by support to attain digital technologies when customers do not have them, should be prioritised.

Some customers, particularly older people, are forced to transition to online banking before they have the appropriate digital literacy training or even access to appropriate technology (e.g. smart phone and laptop).

**Employee training- improved customer service**

It is vital that employees of banks are well versed in how to identify financial abuse and also how to respond appropriately. It is evident from our experience that the standard of employee knowledge on financial abuse varies between banks and within banks. Responses can often be inadequate with staff not identifying the abuse nor acting quickly or appropriately to concerns raised by customers in these contexts. For example, if a customer approaches bank staff saying they think their son is stealing from them, swift action is required, the account needs to be paused and the perpetrator's access blocked (Our Law Centre staff have witnessed some banks do this effectively).

Section 4.1.4 of the Industry Guideline (ABA) requires that when customers inform the bank that they were subjected to financial abuse they escalate the issue quickly and take action to preserve funds.[11] Section 4.4 of the Industry Guidelines also states that banks should *have training programs in place to equip staff with the knowledge and skills to help customers when there is either 'disclosed' and or 'suspected' financial abuse.*

An Australian Law Reform Commission report into elder abuse said, "Training staff was the most commonly suggested step in the inquiry, with some stakeholders submitting that such training should be mandatory."[12]

There have been instances where bank employees have not been sensitive and disregarded an older customer's expressed preference not to set up online banking, or where older customers have advised the bank employee, they are unable to operate online banking. In worst case scenarios, a bank employee appears to be aware that the details provided to activate the online account do not belong to the older customer but the person assisting them. We would suggest that bank employees should be sensitive to customers who express a preference not to use digital banking and respect the customer's wishes by providing alternative options.

**Forms and documents to become a third-party signatory/authority to operate**

When the perpetrator of financial abuse is a third-party signatory to the account or the enduring power of attorney, it is easy for them to steal money. With the absence of a staff member or witness when authorising a third-party signatory on an account, this process is open to being fraudulent, or the customer being coerced into signing it when they do not want to or before they have had the chance to fully understand the implications of this decision.

[11] Preventing and responding to financial abuse (including elder financial abuse) Banking Code of Practice.
[12] Elder Abuse – A National Legal response, 2017, https://www.alrc.gov.au/wp-content/uploads/2019/08/fr131_09._financial_institutioning.pdf.

The Australian Law Reform Commission included this in their paper titled "Elder Abuse: A National Legal Response":

*"For example, banks might require that an employee of the bank, and perhaps another person, witness the forms being signed. This might make it more difficult to submit a fraudulent form. The additional formality may also discourage the person given authority from later misusing the funds. These people might also be required to sign a declaration or* ***undertaking that they will not misuse the arrangement, such as for their own benefit."***[13] Additionally, *The National Older Persons Legal Services Network said that third party authorisations "ought to be considered as seriously as any other substitute decision making instrument."*

We acknowledge the difficulties in this process given the continuing absence of physical branches in some areas which may make this prohibitive. However, the current approach is leaving room for exploitation and customers would benefit from better education and support when determining whether they need a third-party signatory to the account. Furthermore, requiring the third-party signatory to sign a declaration that they will not misuse the arrangement for their own benefit, could provide for a deterrence and also a means for the customer to recover misused funds. A Justice of the Peace could be a witness for both the third-party signatory form and the declaration as well. Appropriate penalties for any misuse of their access by the third-party signatory should be instituted and any potential signatory informed of the penalties prior to becoming a signatory.

**Voluntary income management measures**

Banks need to provide better education and awareness about the variety of options available with account management that limits the types of transactions and amounts that can be used such as opting into protective management measures such as

- 'two to sign',
- pre-set limits,
- getting transaction notifications,
- using dedicated cards and PINs for those authorised to access their banking and
- limiting the type and amounts of transactions or amounts as some ways to protect their banking.

Currently these options are not widely promoted to older customers and are subsequently underutilised. These measures would better protect customers from financial abuse. These options relate to section 4.1.2 of ABA Industry Guidelines on helping customers to manage their own finances which includes "limits on the types of transaction and/or amounts." [14] Section 4.1.2 also suggests options for limiting the type of transactions used for some customers.

**Vulnerable Person's Unit within bank**

We strongly recommend that all banks have a Vulnerable Person's Unit as this would assist financial abuse victims and the services that support them. Some banks already have this function; including BankSA.

[13] Elder Abuse – A National Legal response, 2017.
[14] ABA Industry Guidelines

Staff in a Vulnerable Persons Unit would advocate on behalf of the customers and provide tailored support for circumstances like financial abuse. Staff from services like our specialised Elder Abuse Unit could provide the Vulnerable Persons Unit, within the bank, information about the customer who is experiencing financial abuse (e.g. our staff could inform the bank that money has been stolen and the account needs to be paused). This would not require the bank to share any confidential information about their customer to the external service provider as this would not be necessary. This is an important distinction as this eliminates the security risk to customers.

As highlighted above, provisions in the Privacy Act make it harder for the bank, and in this case, a Vulnerable Person's Unit, to engage with support services and customers, and protections should be made for banks in circumstances where financial abuse is suspected.

**Greater awareness of existing support**

Some banks have implemented elder abuse programs and support, but the awareness of these services is low amongst customers and wider community. Although we cannot speak to the effectiveness of these programs, we believe greater awareness is needed (beyond online advertising) so that any support that is available is optimised.

## 4. Steps that might be taken to support banks to better detect and respond to financial abuse.

Please refer to information above under section one and two.

## 5. The role of government agencies in preventing and responding to financial abuse.

The government can lead early intervention and prevention strategies by increasing awareness of financial abuse and providing sufficient funding for support services that assist victims of financial abuse. There is currently a lack of adequate funding to run civil litigation matters for victim survivors of financial abuse, particularly elder abuse, to reverse or claim damages from perpetrators.

The federal government can also lead by example by making services accessible for a variety of demographics. Other government agencies like My Aged Care and Services Australia are now predominantly digital platforms despite the age demographic of customers being disproportionately unable to access online technologies. This means older people are 'forced' to depend and rely on relatives/supports/carers/informal supports to interact with government agencies through digital platforms and this increases risk for financial elder abuse. Government agencies should be accessible to older people and not require older people to rely on others to access their digital platforms if phone lines and face-to-face appointments are inaccessible.

## 6. The funding and operation of relevant advisory and advocacy bodies.

Funding for relevant advisory and advocacy bodies is crucial. There also needs to be support and training implemented for the workforce in banks that will be responding to financial abuse and other forms of abuse that often intersect.

Services like our Specialist Elder Abuse Unit provide support to some of Australia's most vulnerable customers by assisting those experiencing elder abuse. Access to such support is vital for assisting victims of financial abuse.

## Conclusion

We appreciate the opportunity to provide a submission to the Parliamentary Joint Committee on Corporations and Financial Services inquiry into financial services regulatory framework in relation to financial abuse.

We believe banks should have a responsibility to do more to prevent and respond to financial abuse. The transition to online banking has made more customers vulnerable to financial abuse, particularly older people, and protective measures must be put in place to prevent and respond appropriately.

**Case studies**

Case study 1:

Frank* is in his eighties and has three children and has been caring for his wife who had cancer. Franks son asked whether he could borrow $50,000 and he refused. After his wife recently died, Frank's son told him he had borrowed $50,000 and that he had sought permission from his mum before she died, even though she had very little communication abilities. The son was able to do this without Frank's permission because Frank had given the son some bank details previously for him to set up online payments. Our Elder Abuse Unit advised Frank to get in contact with his bank and ask them to contact our service lawyer. Frank was told the son was able to access the money through electronic transfer as he is a third-party signatory to the account. Thankfully the son eventually paid the money back but in a lot of cases we see this does not happen and recovering the money is very difficult or unattainable.

Case study 2:

Helen* was living in an aged care home with significant health issues that had made her bed ridden. Due to recent changes to her banking, she had to pay her bills online but was unable to navigate this herself. She sought the help of her carer at the aged care home to help her pay the bills. The carer then stole $30,000 without the client's knowledge. The carer had set up the online bank account so that the codes for logging in to the account were sent to her phone so Helen could not access the account. Eventually, after Helen died, the ASU was successful in forcing the return of the funds. However, due to the absence of a registry of unregulated workers, it remained possible for the carer to be re-employed by another aged care facility.

Case study 3:

Mark* was an elderly client of our Elder Abuse Unit. Due to an acute mental health condition, a guardian and an administrator were appointed as his key-decision makers with the guardian making the decision to accommodate Mark in a locked ward. After several years being forced to reside in the secure facility, he was reassessed and found to have cognitive capacity. As such, Mark was once again allowed to control his own financial affairs.

When Mark attended his local bank after many years, he was not allowed to withdraw his own funds as his driver's licence had expired and the bank was not able to formally identify him. The process to remove

the block on Mark's account was extremely difficult; he had to attend in person several times and faced continual barriers with the staff not taking the matter seriously. A staff member from our Elder Abuse Unit attended the bank with Mark, and after many hours the bank reversed the block, but it was a very complicated process. If Mark lived in a regional location with no access to face-to-face banking, it would not have been possible to complete this process online.

Case study 4:

*Edward had credit card debts and wanted to consolidate his loans. He attended a branch for a reverse mortgage. He told the employee he did not know how to use internet banking. The bank staff member took down the email and phone details of the person who accompanied Edward to the branch after Edward said that he could not use internet banking and where it was apparent that he would have to trust his companion to access internet banking to activate the cards. That person activated the account without Edward's knowledge and was able to withdraw all available funds to the reverse mortgage within a short period of time. This meant Edward did not have the benefit of the funds and never had control or use of the cards associated with the credit facility, despite the bank being put on notice that Edward did not know how to use internet banking and the mobile and email address being provided in order to activate his accounts did not belong to Edward.

*names changed for privacy