CHOICE

PASSING THE BUCK:

how businesses leave scam victims feeling alone and ashamed

May 2024

About us

CHOICE is the leading consumer advocacy group in Australia. CHOICE is independent, not-for-profit and member-funded. Our mission is simple: we work for fair, just and safe markets that meet the needs of consumers in Australia. We do that through our independent testing, advocacy and journalism. To find out more about CHOICE's work visit www.choice.com.au

CHOICE

CONTENTS

This report was authored on Gadigal land. CHOICE acknowledge the Gadigal people, the traditional custodians of this land on which we work, and pay our respects to the First Nations people of this country. CHOICE supports the First Nations people's Uluru Statement from the Heart.

INTRODUCTION

Scams are currently one of the biggest problems consumers face. Scams cost Australians $2.74 billion in 2023.[1] In 2022-2023 over half a million people living in Australia experienced a scam, an estimated 2.5% of the population.[2] Scams are becoming more complex and increasingly difficult to identify. Nationally representative research from CHOICE found that 88% of people believe that scams have become more sophisticated or harder to spot recently and that 79% of people fear that other people in their life might not spot a scam.[3]

The size of the problem and the corresponding toll scams are taking on consumers has not resulted in a comparable response by the businesses enabling the criminal activity. The businesses with the technology and resources to detect, prevent and respond to scams are not doing enough to protect consumers. Consumers are left to bear the cost of scams, with only 2 to 5% of losses getting reimbursed across the big four banks in the 2021-2022 financial year.[4] Pathways to redress can be convoluted and unclear, with scam victims left feeling unsupported, overwhelmed and not knowing who to contact.

Passing the Buck: how businesses leave scam victims feeling alone and ashamed tracks the journeys of victims of bank transfer or debit card scams, during the scam and the aftermath, including the financial and emotional impacts, the factors that prevented action and the impact of various responses from banks. This report draws on both quantitative survey-based research and qualitative open-ended answers from respondents. It highlights that victims are left feeling alone and ashamed carrying the burden of scams, while the businesses facilitating the criminal activity of scammers face virtually no consequences.

Anyone can be scammed, especially during a vulnerable moment More than half **(55%)** of victims felt busy, stressed, tired, anxious, distracted, lonely, sad, depressed and/or were grieving in the days leading up to the scam

OVERVIEW: THE LIFECYCLE OF A SCAM:

Before the scam: Anyone can become the victim of a scam, especially during a moment of vulnerability. More than half (55%) of research participants felt busy, stressed, tired, anxious, distracted, lonely, sad, depressed and/or were grieving in the days leading up to the scam.

The scammer makes contact: It can take just one interaction to lead to someone being scammed. Around one third (30%) of respondents had just one interaction with the scammer.

The scam occurs and is identified: In most cases, the victim's bank failed to alert the victim about the scam before the victim realised they'd been scammed. Only 14% of respondents indicated that the bank alerted the victim about the scam first.

The victim decides what to do: Many respondents felt ashamed of the fact that they were scammed and felt hopeless about the situation. Once the scam had been identified, just over half (54%) of people contacted their bank about the scam.

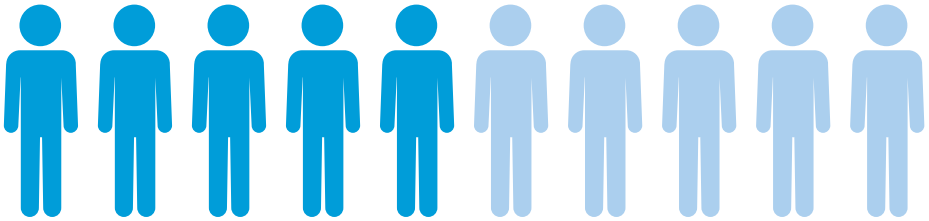
The banks' response: After contacting their bank about the scam, the bank helped try to recover the money half of the time, for just 52% of victims. A key finding revealed by this research is also the inconsistency in the way victims are treated by financial institutions, the outcomes achieved, and their experience of support, or lack thereof. This inconsistency is present across all stages of the process, including prevention, notification, recovery and compensation, and is unfair on consumers. Currently, it seems to be a roll of the dice in how a scam victim will be treated and the kind of support and redress they will have access to.

The impact on the victim: Consumers feel ashamed and unsupported, both as the scam plays out, but also for potentially long periods afterwards. More than half (54%) said the scam had negatively impacted them personally and 61% said they had lost confidence in doing financial transactions online. Being scammed can result in negative effects that are severe and long-lasting, with many respondents saying the experience damaged their ability to trust people. Losses from scams can be devastating in multiple ways, financially and emotionally, and can leave victims feeling traumatised.

Harm and impact on consumers as a result of banks' poor safeguards against scams

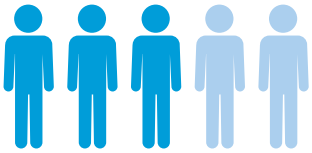
81% of people reported that their bank failed to flag a potential scam before a transfer was made.

In only **14%** of cases did the bank contact the victim to alert them to the scam, after it occurred. In most cases **(79%)** the scam was identified by the victim or victim's family.



After contacting their bank about the scam, the bank helped try to recover the money half of the time, for just **52%** of victims.

Half of the victims **(49%)** believed a 24-hour delay on transfers could have prevented them losing money



Three out of five **(61%)** said they had lost confidence in doing financial transactions online.

69% of people who didn't get reimbursed didn't feel that there was enough support from the banks, whereas only **28%** of people who were reimbursed felt there wasn't enough support.

Recommendations

1 Strong, mandatory and enforceable rules for businesses.

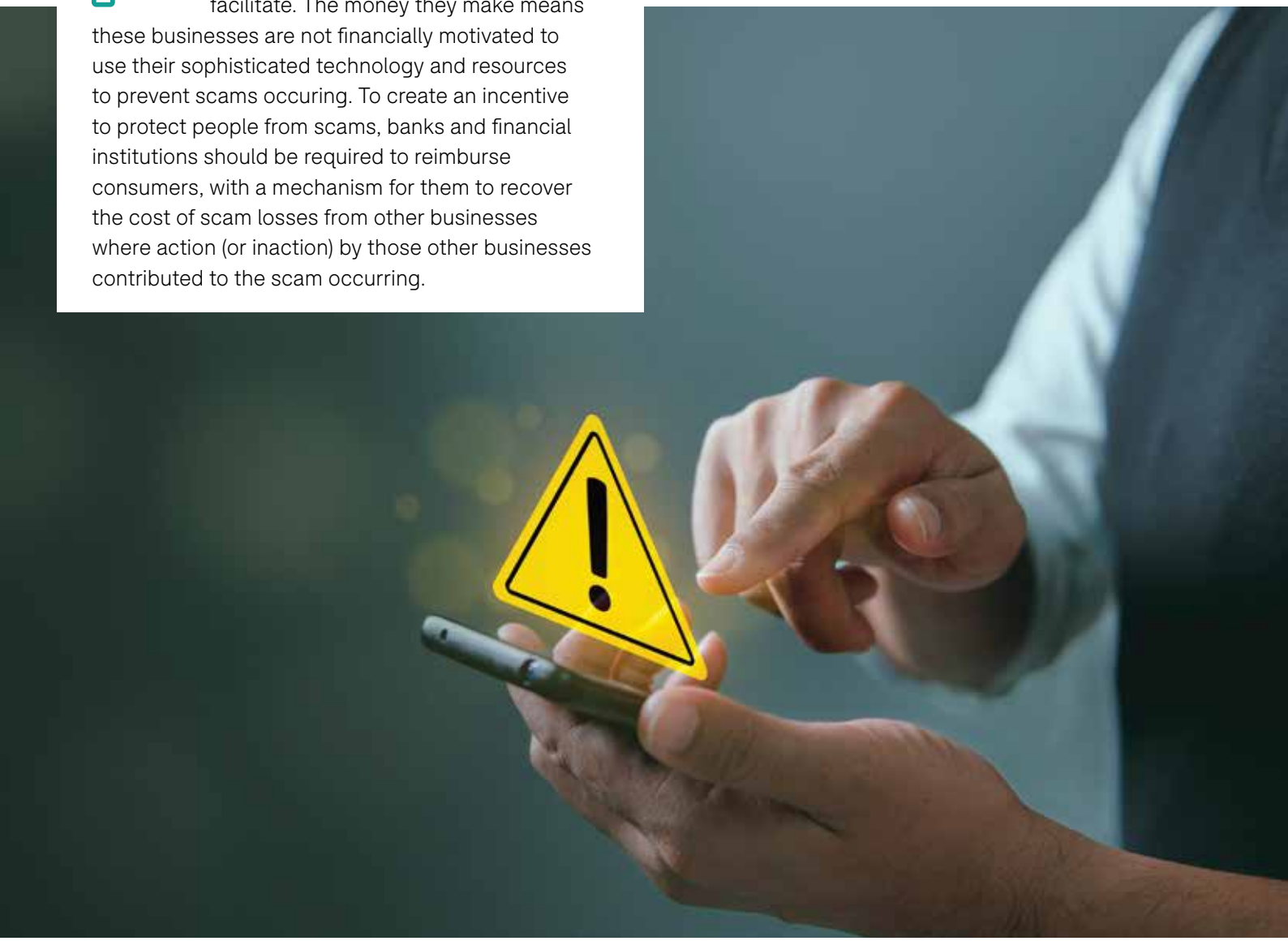
Consumers deserve a high minimum level of protection from scams as well as support and redress if they fall victim to a scam. Currently, the experience for consumers is very inconsistent and depends on the individual businesses involved in the scam lifecycle. The minimum protection consumers receive should not vary in this way. To ensure a high minimum standard, strong mandatory and enforceable rules should first be applied to banks, telecommunications platforms and digital platforms, with other industries included over time.

2 Consumers should be reimbursed for scam losses in most cases.

Many businesses enabling scams make revenue from the criminal activities they facilitate. The money they make means these businesses are not financially motivated to use their sophisticated technology and resources to prevent scams occuring. To create an incentive to protect people from scams, banks and financial institutions should be required to reimburse consumers, with a mechanism for them to recover the cost of scam losses from other businesses where action (or inaction) by those other businesses contributed to the scam occurring.

3 Consumers should have a fair, simple, fast and effective pathway for reporting scams and obtaining redress.

This should include a single door for the consumer to access external dispute resolution. This will improve the experience for scam victims and may increase scam reporting. More reporting of scams should help disrupt and prevent a greater number of scams as these reports provide businesses with intelligence that they should be required to act upon and share with other businesses in the scam ecosystem.



THE LIFECYCLE OF A SCAM

Before the scam

Everyone can be vulnerable to scams

Anyone can become a victim to a scam. Often all it takes is a moment of stress, anxiety or distraction. The UK Consumer group Which? refers to this as being beyond the "emotional 'window of tolerance'"[5], when someone is especially stressed, tired or distracted. Scammers know how to target the weaknesses of their victims and exploit moments of vulnerability.

These situations are unavoidable as everyone gets busy and stressed. It is not acceptable for anyone to be left to the mercy of scammers. Consumers deserve to be protected by the businesses and services they use, trusting that those companies have their backs, even when vulnerable. CHOICE's research indicates this is not consistently happening right now. There are no public policies, rules or regulations to establish a baseline. This means that – despite many scams being similar and following a pattern – protections against scams vary business to business, as do the businesses' responses to scam victims.

Scammers exploit moments of vulnerability

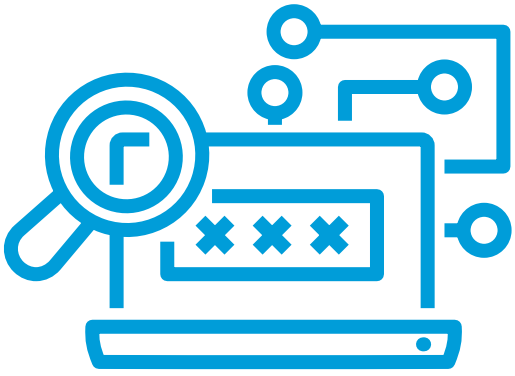
More than half (55%) of research participants felt busy, stressed, tired, anxious, distracted, lonely, sad, depressed and/or were grieving in the days leading up to the scam. This is also reflected in the open-ended comments given by respondents:

"I felt foolish that I had fallen for the scam. The text supposedly came from my daughter asking for me to transfer money to pay a bill. Normally I would have found this suspicious, but they contacted me on a Thursday, and my daughter was receiving chemotherapy every Wednesday and was often very ill each Thursday. When she was in hospital, I would pay bills so that she didn't have to worry about them, so when I got the text, I thought she was laid up with nausea and I jumped into Mum mode to "help out". If it had been any other day, I would have queried it."

"I was a victim of Lismore floods, we were all getting scammed one way or another. I thought that I would never get scammed, but now I don't answer phone calls, delete emails, transfer as least as possible, no pay ID, use cash as much as possible. There is a new scam every day."

For some, aspects of vulnerability like disability, lower English skills and unfamiliarity with technology are permanent and ongoing. Scammers target community members likely to be consistently more vulnerable to scams. Accordingly, this means that the obligations on industry and the presumption of reimbursement must be higher for vulnerable consumers.

The average age of survey respondents for this research, who were all victims of bank transfer and debit card scams, is higher than the actual population. Older consumers can be more vulnerable to scams. The age group of 65 or older also had the highest reported losses in the Australian Competition and Consumer Commission's (ACCC) ***Targeting Scams 2023*** report.[6]



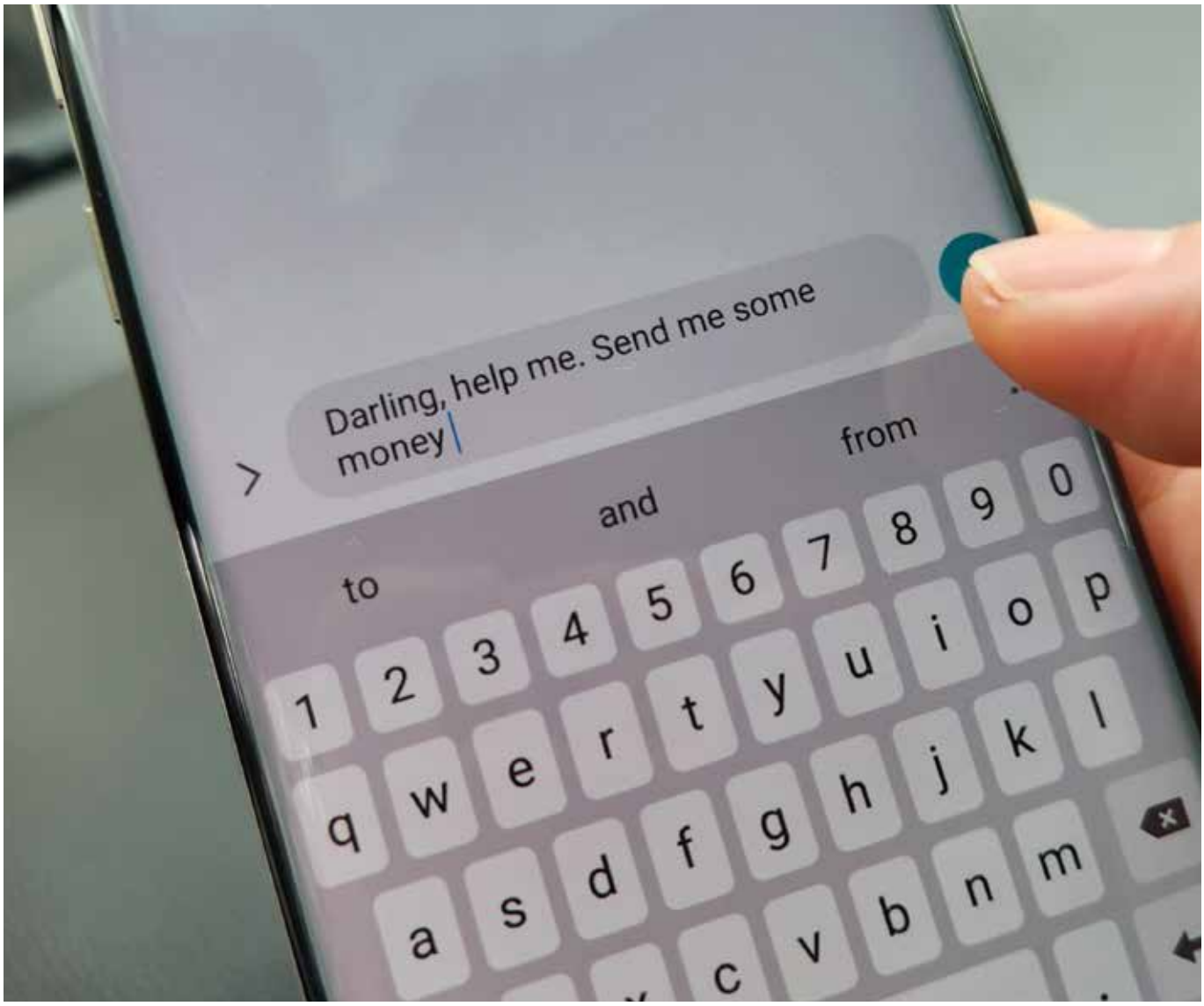
CHOICE research respondents also included people who live with ongoing vulnerabilities that may have contributed to them being targeted by a scammer. For these people, the impact of the scam was also often worse:

"I am a disabled pensioner, considering I realised and reported the scam within four hours and gave a lot of detail to the fraud squad of the bank and then only to get $50 back is shocking. I would of rather got nothing then have the insult from the bank to give me $50. The money was everything I had at the time and incredibly I still have the person's email address yet they cannot do anything. That is crazy."

"The money scammed was from my disabled, hearing impaired 20 year old. When we contacted ING, they took no action to recover the money for two days. Eventually after her Dad advocating for her and threatening to contact the ombudsman, ING offered a one off payment. We accepted because of the impact the scam and ING was having on her already poor mental health. It was disgusting because ING could see that her source of income was her disability support pension and took advantage of her being a young disabled person. They accepted no responsibility for their lack of action."

Consumers are aware of the threat that scams pose to their friends and family. Nationally representative data from CHOICE revealed that almost 8 out of 10 people fear for other people in their life that they might not spot a scam.[7] Scam protections must be strong enough to ensure that Australia's communications and financial systems work for all members of society, no matter what level of vulnerability they are currently experiencing.

"My elderly (89) mother was befriended on whatsapp by someone pretending to be me. They said I'd damaged my phone and needed her to help by transferring some money to a few people they said I owed money to. They began with a couple of small amounts to test if she would do it and kept them under $100 so she didn't need to include authorisation codes. They then scaled this up to two much larger amounts. She was visiting a country relative at the time and so wasn't in my house. She tried to contact me to verify the need, but the scammer had convinced her that I'd changed my phone to a new number and to delete my old number from her phone contacts list. She eventually called my daughter to ask if I was OK and why did I owe others so much money which of course I didn't. This alerted us to the scam and so she went to the local rural Westpac branch. They told her she needed to drive to Melbourne and confront me and be sure I hadn't instructed her to do the bank transfers before they'd investigate."



The scammer makes contact

Businesses allow scammers to exploit their systems to contact victims

Many businesses are not currently subject to mandatory rules for responding to scams and scam victims. This results in inconsistent and varied responses to scams, approaches to anti-scam strategies, and generally poor outcomes for victims. Businesses should be subject to high standards that are enforced by well-resourced regulators to ensure a baseline of protection, prevention and support for all consumers in Australia.

It can take just one interaction to lead to someone being scammed. Around one third (30%) of respondents had just one interaction with the scammer, and for 16% it was done without contact. For the remaining respondents:

34% were contacted a few times, e.g. 2 – 5 interactions	**14%** had many interactions, e.g. more than 5 times in total	**6%** had continuous interactions, e.g. multiple times a week

New scams emerge constantly and use sophisticated technology and past learnings to manoeuvre past protections that may have worked previously. The fact that only one interaction was enough for almost one third of victims to be scammed reinforces the unfairness of expecting consumers to be solely responsible for spotting and protecting themselves from scams.

"I did a huge amount of research but still got scammed. The false websites, verbal communications, verbal and written documentations. This was a very well constructed scam. I could have lost much more."

"The scam was very professional and caught many in my social circle, including accountants and other sophisticated investors. The company was not on the ASIC [Australian Securities and Investments Commission] website as a scam, people involved in the investment are not fools and they also did numerous checks. It was only after I asked to just do a trial withdrawal of a portion of the amount invested that I became concerned (as it was taking so long), this coincided with other investors having similar difficulties and finally having their account locked and phone calls not returned."

Several respondents noted that official bank phone numbers were spoofed by scammers, so that calls or text messages from the scammer appeared to be from the victim's bank.

"My credit card had been compromised 4 times in less than a year. The bank would call me to tell me that there were suspicious transactions and would cancel the card and send a replacement. ANZ use a text message system to verify that you are speaking with an ANZ officer. Late on a Friday afternoon I received a call from 'ANZ' advising that my card had been compromised. My immediate reaction was 'not again!' I asked for proof of ID and I received a text message through the usual message thread to confirm I was speaking with an ANZ officer. From that point on I believed I was speaking to my bank. The person gave me his name and said he was with the international fraud team. It's changed now, but at that time they had contact numbers on the ANZ website, one was a 24 hour international contact number. Since I was in front of my computer I looked at the website and saw that the number he was calling from was the same."

Digital platforms and telecommunications platforms are also being used by scammers. In 2023, text message and phone calls accounted for 54.70% of scam contact methods and $142.90 million in reported losses. Internet and social media accounted for 11.64% of contacts and $163.20 million in reported losses.[8] In 2023, Scamwatch reported a 249% increase in losses to social media scams since 2020.[9]

18% of respondents in our research were contacted by the scammer by phone or SMS and 51% were contacted via a website or social media platform. Of social media platforms, Facebook was the top platform (66%) that scammers used to contact victims.

"Twice I have been caught with an advertisement on Facebook using well known personalities making recommendations. Apart from a loss of money it has taught me to be very careful of any advertisements on Facebook. Too many fake identities."

"I ordered products from online stores that appeared in my Facebook feed. They looked legitimate and the products were ones that I had seen but they were never delivered despite a very realistic tracking system that appeared to show that they had been delivered to my letterbox. Upon contacting them they eventually offered me a 30% refund but even that has never eventuated. A very complex and sophisticated system that must have them raking in a lot of money."

"The scam started with a text message to my wife, purportedly from her daughter, saying that she had dropped her own mobile into the toilet and was using a work colleague's phone. The text said that "she" needed $600 urgently to buy a new phone, and that she's already arranged to pick one up. A good reason for the urgency was given but I don't recall what it was. The text gave details of the account to pay into. My wife was about to go into a doctor's appointment, so she sent me a text asking me to make the transaction. So of course I paid from my own account - it wasn't possible to check with her daughter (we thought) because of the lost phone. It was only after my wife got home that she called her daughter who obviously was totally unaware of any text. I remembered (too late) the strange BSB number, and that I had accepted it because I was getting the information secondhand. I immediately phoned RACQ bank. They were very helpful, and managed to retrieve the money within about 6 hours."

Many respondents from CHOICE's research were scammed by fake product and service scams: one in two (49%) people fell victim to a product or services scam. For the calendar year of 2023, research from the ACCC found that over 16,000 people reported losing money to a scam that started on a social media platform or an online forum with an ad, a post, or a message.[10] Many of those people reported placing an order, often after seeing an ad, but never received the products ordered. Some reports described advertisements that impersonated real online retailers.

A 2023 CHOICE investigation[11] revealed that platforms such as Google, Facebook and Instagram were rife with scam ads promoting likely fake websites for some of Australia's most popular retailers. The investigation also found issues with Google's own policies to prevent scams because some advertisers did not appear to be verified before they published ads. Facebook's advertising policy in Australia only requires verification if an advertiser is running political, social issue or electoral ads.[12] Users do not need to be verified to post listings on Facebook Marketplace. A recent analysis by fraud experts in the United Kingdom concluded that a third of ads on Marketplace in the UK "could be scam posts".[13]

It is clear that digital platforms and telecommunications companies also have a key role to play in protecting consumers in Australia from scams. Strong, mandatory and enforceable rules for these businesses will help ensure consumers can expect and receive a high minimum standard of protection from scams, including, for example, meaningful verification of whether advertisers on digital platforms are legitimate. Making sure consumers are reimbursed for most scams will also financially motivate businesses like digital platforms to do more to disrupt and prevent scams. Currently, digital platforms have a perverse incentive not to act on scams because they generate advertising revenue.

Scammers succeed despite consumer efforts to avoid scams

About half of the respondents to this research took measures to verify if they were being scammed, including trying to check the identity of the person who contacted them before they knew it was a scam (53%), and checking the website or the URL before they knew of the scam (47%). Many respondents said that the scammer made them feel under pressure. Scammers can create vulnerability themselves by causing stress, and often make people feel a sense of urgency.

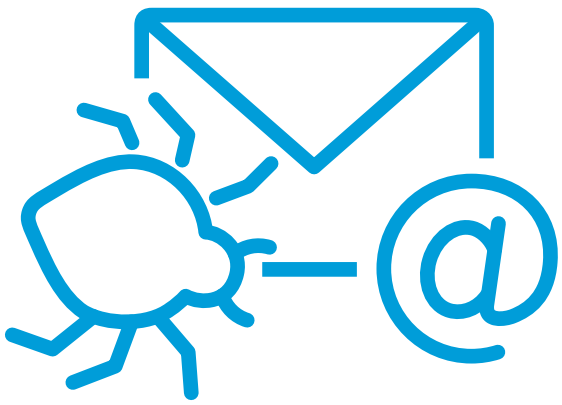
"The scammers were on the phone trying to convince me that I needed to transfer money to stop the bank from losing it... the man on the phone was persistent for several hours. I felt overwhelmed & stressed as I had a very small amount of savings and didn't want to lose it. I still can't believe I was sucked into it... I never told my family."

"Everyone I speak to is stressing about scam texts, phone calls or emails because they are becoming smarter and more complex. I have always considered myself very careful and can't believe how I got taken for a ride particularly with my mum's money. All family members are sympathetic and supportive and it has made everyone be aware of extra caution."

"Aged relative felt they needed to earn some money to be more financially secure. Conned into options online trading... She was convinced by a slick salesman and daily pressure phone calls that online options trading was a way to supplement her pension. We only found out about this because someone was staying with her and had taken some of the abusive phone calls and he gave them a piece of his mind. She swore him to secrecy but he did tell us in the end. The reasons she gave for doing it are that she found it exciting and it kept her mind engaged, these guys are really good."

Scams are becoming more sophisticated and harder to spot. Scammers are able to spoof bank numbers and SMS IDs, invoices, relatives' voices and more. Expecting consumers to be constantly aware of current and emerging scams at all times is unrealistic and unfair.

Consumers are aware that they need to be on the lookout for scams, and yet scams still take place. Consumer education will never be a complete solution. Businesses must be subject to strong, mandatory obligations that impose high standards of consumer protection against scams. Large sophisticated businesses must use their knowledge and resources to act against scams, instead of enabling scammers to operate on their platforms.



The scam occurs and is identified

The role of banks and financial institutions in stopping scams

The bank or financial institution should always be the first business a consumer goes to for help. The financial institution is the only business that could prevent the money from being transferred and is best placed to stop a transaction to get a victim's money back. The financial institutions that facilitated the loss of money are also best situated to detect scams and warn consumers at the crucial moment.

Focusing on banks and financial institutions also simplifies the process for consumers, who should be able to be confident that reaching out to their financial institution as the first step is the best action to take. Ensuring every part of the reporting and redress process begins with, and flows through, a victim's bank is the simplest way to achieve better consumer outcomes. A consumer should not be passed from telco to bank to digital platform and be forced to negotiate through multiple instances of internal dispute resolution. This would cause stress and fatigue, as well as creating more bureaucracy within the system.

Banks play a key role in enabling scams

81% of people in our survey reported that their bank failed to flag a potential scam before a transfer was made. Almost 3 in 10 (27%) people said that their own bank helped organise the fraudulent transaction either in person, online or via phone. Increasing friction, such as transaction delays, could potentially help address this. Half of the victims believed a 24-hour delay on transfers could have prevented them losing money.

"I was told that it was my duty to assist the Telstra/ AFP sting and to transfer money via Western Union so they could arrest the scammers. Very ironic! I did what they said to do twice but then I began to feel like it was a scam. They then locked up my computer so I went to the bank to find out what had been done to my account. I was horrified to see that there was a pending amount of $7,000. When I told the manager to stop the payment going through she told me that she couldn't. I was furious when I received a letter from CBA declining my request for reimbursement and stating that I couldn't appeal."

"The banks should offer support to those who have been scammed. There are no guarantees from banks that they will reimburse losses yet they want everyone these days to do everything on [the] computer."

"My dad had been talking to the builder the next day after I had sent the money and mentioned I'd made payment. The builder said he didn't receive the receipt of payment from me. The hackers [scammers] had also intercepted that email from me. The builder then contacted me to alert me."

"When things did not evolve as promised and paying out several tens of thousands of dollars - my partner looked up their business online and found out that this is a scam, amongst a long list of many such scams."

Banks are failing to identify scams quickly

Once the scam occurred, in most cases, the victim's bank failed to alert the victim about the scam before the victim realised they'd been scammed. Only 14% of respondents indicated that the bank alerted the victim about the scam first, whereas 79% of respondents said they or their family identified the scam, and 7% were contacted by another source.

"Made me angry that the banks did not stop the payment as it was easy for them to check if it was fraudulent."

The victim decides what to do next

Shame, and the belief that banks won't help, stop victims reporting scams

Many respondents felt ashamed of the fact that they were scammed and felt hopeless about the situation. Once the scam had been identified, just over half (54%) of people contacted the bank where the money was sent from during the scam (their own bank). Those who did not contact their own bank did not do so because they felt like it was their own fault (30%), they didn't think the bank would help (29%) and it didn't occur to them that the bank could help (16%). A further 16% said they tried but it was too hard to report.

"[who did you tell?] No one. Embarrassed and didn't know who to contact. There was no chance of retrieving the money."

"I felt really stupid and lost confidence for 6+ months on trusting anyone. Didn't want to tell anyone due to embarrassment."

"The person involved hid in the bedroom for 2 days after being scammed and didn't say anything to anyone. When it was realised that she had been scammed the husband and daughter tried to get information from her as to what went on and she was too embarrassed to tell and it took a day or so to get the details. When the scam was reported to the ANZ he dealt with several different people and departments and spoke to very junior staff in the scam section who couldn't/didn't know how to handle it and passed it on. She lost $67,000 and was given $6,500 as recompense."

"Scam websites look so much like the real thing. Sometimes difficult to tell. Makes me less confident about paying things online. Worried that scammers pretend to be the bank. Very nervous about my bank account. Bank said it was my fault. I thought I was paying a Linkt bill. Made me very embarrassed to be so stupid but I tell people so it won't happen again. But I'm still worried that I may fall for another scam sometime."

Not reporting scams quickly to the bank reduces the likelihood of money being recovered. The shame and stigma felt by those who have been scammed can prevent reporting as many people don't want to report the fact that they were scammed. Incomplete reporting hampers efforts to prevent scams as a key channel for disrupting scams is via businesses and government sharing information about scam reports efficiently, and acting on the information received.

Consumers are left alone to carry the burden of scams, and this is clearly felt among victims. The onus of responsibility on consumers and narrative around shame and embarrassment can cause acute emotional distress. Much of the messaging around scams is about being educated and alert, so when someone is scammed they feel as though they've been foolish. Shifting messaging to focus on what to do immediately after you've been scammed, and acknowledging the sophistication of scams, would potentially help alleviate this.

Victims who reported the scam to a bank are frustrated by the process

If a victim does decide to talk to a bank, there is no guaranteed pathway to redress. Respondents reported long wait times, confusing processes and a lack of follow up. This is reflected in the 2023 Australian Securities and Investments Commission (ASIC) report ***REP 761 Scam prevention, detection and response by the four major banks***, which found that "for three of the banks, we saw information indicating that their staff resourcing levels and capability had not kept pace with the increasing volume and sophistication of scams."[14]

Many victims of bank transfer and debit card scams are finding banks' scam reporting systems hard and confusing. 32% of CHOICE survey victims did not feel like their own bank's system of reporting a scam was easy and straightforward, whereas 68% of respondents did find it straightforward. This is another example of the inconsistency that scam victims face when trying to move through the process.

"I was on hold music for 80 minutes trying to report the scam and possibly stop the transfer."

"One issue is it took a lot of time to talk to the main person on the phone as you are put through to a number of staff and when this is going on it is too long a wait. You need to talk to someone immediately to stop any transactions happening. Money could be taken while you are holding on the phone. As our accounts are locked we are not sure how much was taken but was told they had stopped some transactions."

"Scammers called me (and other people) saying they are from NBN. They said they can improve my Internet speed. Eventually they got access to my PC and were able to enter my Netbank then to transfer my money to some AMP account. It took me 90+ minutes to reach somebody in CBA security. I don't know what CBA staff did then, but much later I was informed they could not retrieve my money. CBA did not want to compensate anything. They agreed to compensate 50% only after a long and painful discussion. My main argument was I'm their customer for 27 years and CBA never ever had any troubles with me."

"I complained about how difficult it was to get to speak with the right person at both banks. The fact that I was placed on hold for ages and then continually being transferred from department to department. Plus I complained about the fact that Westpac have not taken any accountability for the scam."

A fair, simple and fast dispute resolution pathway for consumers must be established, so that consumers can be confident that no matter which bank they use, they will have access to timely support and redress. This pathway must be clear and easily accessible, and lead either to a resolution or an external dispute resolution pathway within a short timeline. During what is a stressful and traumatic time, the victim should feel confident that they will achieve a solution.

The banks respond

A significant number of responses from banks towards victims are inconsistent, confusing and too slow. Banks often take too long to communicate with the victim, don't follow up and make consumers jump through hoops in order to achieve any outcome.

Banks are taking too long to respond to victims of scams

While 68% of victims got immediate action from their own bank, 32% did not. Time is of the essence in recovering stolen funds, so it is essential that banks respond immediately. Considering that over two in three victims saw an immediate response, it is clearly possible. However, the banks' responses are demonstrably inconsistent. Consumers should be confident that any report of a scam with any bank will be taken seriously and acted on immediately, not faced with a roughly one in three chance that their bank will be slow to act.

Over a quarter of respondents (26%) said they had to fight to have the scam be taken seriously, and 74% did not. When a scam occurs, acting quickly is critical. Banks should be required to respond as soon as possible. One in four victims not having their scam experience be taken seriously is unacceptable.

"Both my parents had multiple accounts subject to scam. My father has advanced dementia and the banks have refused to deal with us despite Enduring Power of Attorney being provided multiple times and simply asking for transactions to be investigated as fraud claims. Became aware of scams on a Friday night and contacting banks was extremely difficult - first to find a contact number, then to speak with a person. Waited hours and possibly more money taken during that time. Banks basically wiped their hands of it."

Respondents say banks are failing to provide contact details of someone who could help the victim when they contacted the bank for their help. 58% were not given the details to contact someone from their own bank to help them, while 42% of victims were. During what is an incredibly stressful period for the victim, banks should be offering support and making the process of seeking and obtaining help as straightforward as possible.

Banks often don't help recover the victim's money

After contacting their bank about the scam, the bank helped try to recover the money half of the time, for just 52% of victims. This is an extremely inconsistent response, and means roughly one in two victims of bank transfer and debit card scams were left to chase their stolen funds on their own. Unlike banks, consumers do not have the knowledge and infrastructure to do this.

Other details of the bank's response also varied significantly. Respondents said the banks recorded that a victim had reported a scam only 41% of the time and for 12% of victims, no one from the bank got back to them at all. For others, the response by the banks often involved other challenges:

- *Eventually got onto the right person or department after being kept on hold and / or passed between departments - 18%*
- *Report of a scam was dismissed by the bank - 12%*
- *Couldn't get through to the right person or department to report the scam - 3%*
- *Other - 9%*

Victims' experiences with banks are inconsistent

Banks' responses to victims, both as the scam is unfolding and after the fact, are inconsistent. 22% of respondents rated their experience with the bank handling the scam as poor or very poor. Less than half (48%) rated the experience with the bank handling the scam as good or very good.

"The bank contacted me to say there was a possible fraudulent transaction, yet they didn't stop the money going. They kept updating it was being investigated and eventually said it was gone. It was only after complaining and stating facts that the bank did not notify me of new payee or large transfer and did not stop funds leaving they agreed to compensate most back."

"Because my identity had been stolen in the medibank loss of data they were able to pretend to be the bank and knew a lot about me and the details of my bank account. They told me they were from my bank and there had been an unauthorised debit from my account and I need to transfer the money to a new account. I felt reassured as they knew my full name, date of birth, address and account number. Although I reported it immediately to the bank, it took over 1 hour waiting on line to do so, it felt like they did nothing for days and then told me the money had gone."

"They claimed that I gave the scammers access to my account, which I didn't do. They followed my key strokes, transferred money from my Isaver account to my credit card and locked up my computer. When the bank showed me that there was a $7000 debit on my credit card I told them to stop payment but they said that only the recipient can stop payment. Even though I was CBA's customer I had no rights. I complained but they rejected my complaint and stated that I had no right of [appeal]."

"If I hadn't acted for my mother at the time the bank would have forced her to pay the entire statement figure including the scammed $75,000. My decision to work it through for my mother meant she had little stress. It was a total waste of time for me though."

Establishing strong, mandatory rules and standards for dispute resolution pathways will reduce this inconsistency and set a bar for scam victim support that all banks must reach.

The impact on the victim

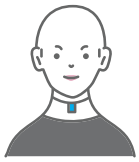
People are overwhelmingly bearing the cost of scams, both financially and emotionally. More than half of CHOICE survey respondents (59%) didn't get any money back from a scam. However, this is not representative of all scam victims. Research from the Australian Securities and Investment Commission (ASIC) found that reimbursement across the big four banks varied but was low across the individual banks, ranging from 2 to 5%.[15] The institutions that consumers trust with their money and their financial security are not providing adequate support.

"I felt embarrassed and ashamed and I don't trust anyone I don't know now. I am reluctant to transact online and have to ring to check before making any transfers. It has left me bitter and angry that Bendigo Bank allowed fraudulent accounts to be opened without identity being checked (police report advised me it was identity theft)."

Most victims negatively impacted by the scam

After being scammed, many victims feel depressed, ashamed and unsupported as they are left hung out to dry by a system that is failing them. The negative effects can be severe and long-lasting. Many respondents spoke about how being scammed impacted their ability to trust people. More than half (54%) said the scam had negatively impacted them personally and 61% said they had lost confidence in doing financial transactions online. In a world where most banking is now done digitally and where some banks do not even have physical branches or do not have a branch in every town, there is little room for consumers who are not confident in online financial transactions.

"Basically, we - my partner and I have become distrusting hermits - we stay home, we are both retired, we trust no one and nothing anymore. And we are so ashamed of what happened, we tell no-one about it, if anything about scammers is ever mentioned."



"Since I have been scammed for my life savings,including my super, I have been hiding in the house and having minimal contact with people in general. I only go out to either work if I am lucky enough to have work, or to buy groceries etc. I had to sell most of my assets and the cars (a car and ute the same model) are from damaged cars that I acquired very cheaply and made them from several damaged ones. My level of trust in humanity has dropped and I have become a recalcitrant. Life sucks."

"Devastating and left the family crying, distressed and living the nightmare thinking that the scammers had all the personal banking and details of the location and could come back anytime."

"I used the ANZ app for the transactions. After the scam the bank advised me to stop doing so whilst they tried to recover the money (4 transactions). The final 10 took 2 months. I then downloaded the app again when the bank told me it was safe to do so. But when I did so the scammers used the app to take 2 transactions of just under $10K my limit of Pay Anyone. Fortunately, I noticed on the day and contacted the bank. The money was retrieved quickly, the bank never apologised to me for not closing a loophole. I lodged a complaint, but have never heard back from the bank about it, except the initial acknowledgement and a complaint number."

Victims reported an overall decrease in many aspects of life after being scammed, such as family relationships, social connections and short term financial comfort (Figure 1). Being scammed is an experience that can have an impact on the victim long after the scam has concluded. Harms are exacerbated when not dealt with correctly by the businesses victims turn to for help following scams, such as banks.

"Hurt financially and seen as a dumb person for falling for it."

"I suffer from depression now from it all."

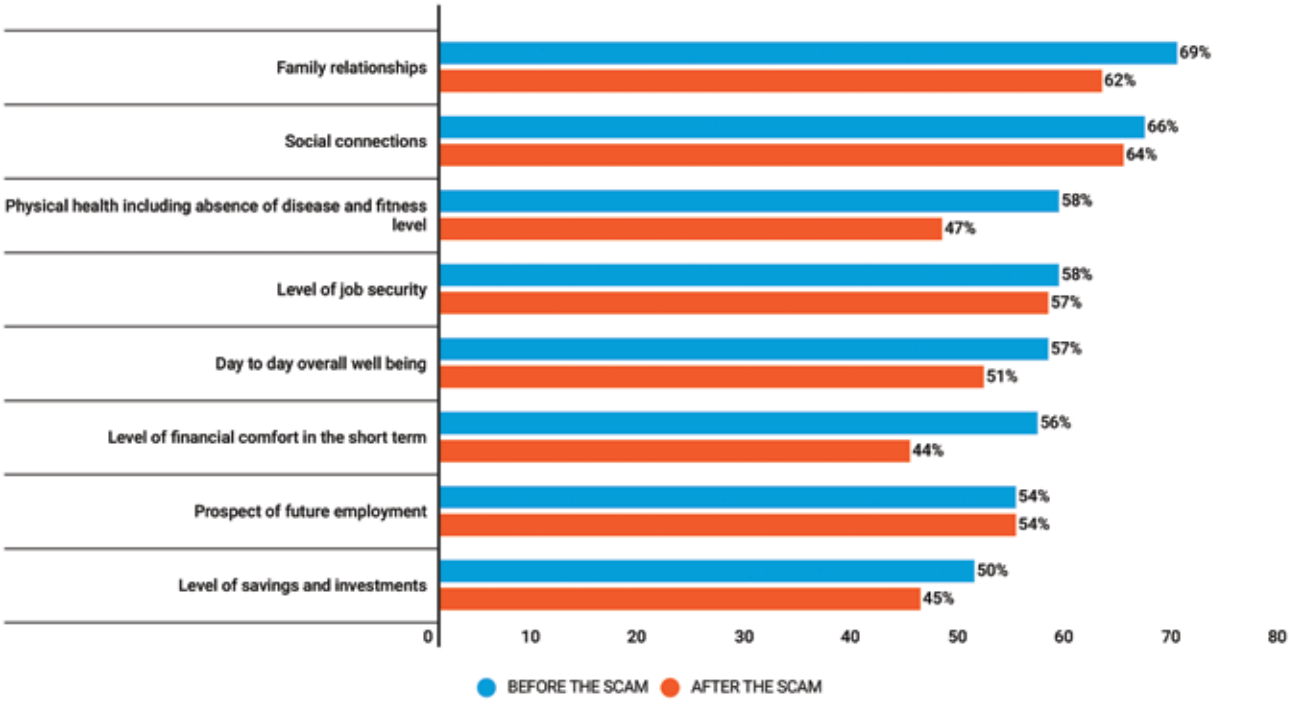


Figure 1: impact of the scam on various aspects of life of respondents

It is clear that current protection and support systems provided by banks do not match the severe impact that scams are having on consumers in Australia. Banks should ensure staff members who are on the frontline of dealing with scam victims are trained to alleviate shame and embarrassment and refrain from victim-blaming.

"I was made to feel 100% responsible for falling for the scam. I recognise that how I feel etc impacts my ability to trust myself when something seems suspect. Once I did answer the call from the scammer the threats made me more and more insecure and they tied up my phone. Sense finally prevailed so, I got lucky and ended the call. Now I do not answer calls from unknown callers. Delete email messages. The scam used Amazon Prime as an in - I'm not sure that Amazon Prime does enough to protect purchasers."

Some victims' trust in banks impacted

As well as having a huge impact on victims, the failure of a proportionate response from banks has the potential to severely impact societal trust in banks. 37% of respondents are less likely to trust their bank after the experience of reporting their scam.

"The NAB told me not to contact them again after 2 or 3 emails. Rude! The banks could totally prevent these scams with account name/number matching. I would love to take NAB to court but how much would that cost? We felt totally let down by the NAB. I often think about what we could do with $152,000 instead of it going to some low life scammer."

Not enough support from banks

Only 1 in 2 (50%) respondents, including those who did not report the scam to a bank, believed they were provided sufficient support from the banks to help them. It is unsurprising that victims are hesitant to report when they are already feeling ashamed and unconfident in the support they will receive.

"Banks need to step up. The current systems have failed to protect consumers and are destroying lives. The $27,000 I was robbed of isn't just a number. It represents a great loss to my family - less free time together because I need to work more, holidays that might have been, sports gear, music lessons, education. Meanwhile - ING and HSBC carry on as usual."

Unsurprisingly, victims who have been reimbursed felt more supported by their banks than scam victims who haven't been reimbursed. Of those who weren't reimbursed, 69% did not feel that there was enough support from the banks. Of those who were reimbursed, 28% still felt there wasn't enough support. Banks still have more work to do to ensure that every scam victim feels supported. There must be clear and enforced rules about banks' obligations to support victims so that every consumer – no matter which bank they belong to – is supported through what can be an incredibly stressful and traumatic experience.

Similarly, victims who weren't reimbursed experienced worse wellbeing, financial and social, and worse loss of trust. 56% of people who didn't get reimbursed reported a negative impact on them personally compared to 48% of people who got reimbursed, and 63% of people who didn't get reimbursed have lost confidence in doing transactions online compared to 56% of people who got reimbursed. The negative impacts even if consumers are reimbursed highlights why no one ever wants to be scammed and why reimbursement is unlikely to meaningfully change consumer behaviour in protecting themselves against scams. In contrast, reimbursement will have a significant impact on business behaviour.

Too many consumers are experiencing poor service when they report getting scammed. Table 1 highlights the widespread inconsistency in the experiences of victims when reporting to their own bank. While some consumers were satisfied with the support they received from the bank, others were not. Currently, it seems like a roll of the dice whether a victim is treated well when they report the scam. Banks must adhere to standards of support and treatment for scam victims so that consumers are not at the mercy of inconsistency and uncertainty.

Area of support	Own bank
Consistency of the advice and explanations	50% said very good + good 29% said fair 21% said poor or very poor
Emotional support	49% said very good + good 25% said fair 26% said poor or very poor
Speed in which the bank resolved the scam (if resolved)	48% said very good + good 24% said fair 29% poor or very poor

Table 1. Breakdown of experiences of support from banks, own and receiving

"Anger at being scammed and embarrassed at not being more careful and felt I should have noticed. Second time in a year that card had to be cancelled and reissued which is inconvenient and also impacts direct debits. Frustration with the length of time on hold with bank to deal with the issue. Concerned about personal data being available to scammer, i.e. mobile number and address."

"My scam involved several bank transfers - both within and across Banks, and purchase of Google Play card purchases etc. We closed 3 bank accounts because of their total lack of interest and accountability in both managing and returning our money. I will NOT use computer bank withdrawals, transfers or transactions at all now. I do NOT trust my own judgement any more and rely on other family member inputs to help me work out possible scams. It's time consuming and a constant reminder of my failure to protect my family's money. Very very traumatic. I've had no further feedback from either police or Banks involved."

RECOMMENDATIONS

This research shows that businesses are getting away with facilitating scammers' criminal activity and facing practically zero consequences, while consumers are left feeling ashamed and alone to carry the burden of scams. It has been left to industry to improve their systems and respond to scam victims, but this has resulted in a lack of action, victim blaming and consumers shouldering scam losses.

It's clear that there is much work to be done to protect consumers in Australia from scammers, but it is important that any updates to the current system and processes result in the best possible outcomes for consumers and bring Australia in line with similar international jurisdictions, with which we are currently out of step.

Several similar jurisdictions to Australia have introduced or are considering reimbursement for scam victims. In 2023, Britain's Payment Systems Regular (PSR) made it mandatory for banks and payment firms to reimburse victims of online bank fraud within five days.[16] All payment firms will be incentivised to take action, with both sending and receiving firms splitting the costs of reimbursement 50:50. This system was previously voluntary, and during that period in 2022 British banks that committed to the Contingent Reimbursement Model (CRM) Code reported a 19% reduction in scam losses on the previous year.[17]

In March 2024, New Zealand's Commerce Minister ordered banks to come up with a voluntary reimbursement scheme for consumers who have been scammed.[18] The European Union (EU) is also updating its Payment Services Directive to include refund rights (reimbursement) for scam victims who suffered losses due to a failure of the name verification service to detect a mismatch between the name and bank account number of the payee, and/or a scammer convincingly spoofing communications from the bank.[19]

Australia must ensure its scam protections keep pace with the rest of the world. Scams are sophisticated financial crimes that do not recognise borders. If Australia falls behind, we risk becoming a more attractive target.

1 Strong mandatory enforceable rules for businesses

Consumers deserve a high minimum level of protection from scams as well as support and redress if they fall victim to a scam. Currently, the experience for consumers is like a game of chance with very inconsistent experiences. The minimum protection consumers receive should not depend on which business is involved. Strong mandatory rules should first be applied to banks, telecommunications platforms and digital platforms, with other industries included over time.

Industry cannot be left to develop their own codes. Industry has so far been left to manage responding to scams and this has resulted in consumers losing billions of dollars a year and experiencing intense harm. Prescriptive standards that cover prevention, detection and disruption are needed, and these must also be able to function as technology and scammers develop and innovate. Security across industries in the scam ecosystem is insufficient, and it is critical that enforceable obligations are imposed on industry as soon as possible to better protect consumers.

2 Consumers should be reimbursed for scam losses in most cases

The businesses enabling scams make revenue from the criminal activities they enable and are not financially motivated to use their sophisticated technology and resources to prevent them. Banks and financial institutions should be required to reimburse consumers, with a mechanism for them to recover the cost of scam losses from other businesses where action (or inaction) by those entities contributed to the scam occurring.

Consumers are overwhelmingly bearing the cost of scams. With little skin in the game, incentive is low for banks and other businesses enabling scams to maximise scam detection and prevention efforts. Current approaches by banks and other businesses are inconsistent and can often be slow, confusing and unsympathetic.

Mandatory reimbursement of consumer losses is the best way to prevent and disrupt scams. It will incentivise adequate investment in prevention systems and ensure consumers can access redress where industry has failed to protect them. It should also reduce both scam losses and Australia's attractiveness to scammers.

3 Consumers should have a fair, simple, fast and effective pathway for reporting scams and obtaining redress

Consumers need a simple, single, fast and effective pathway to seek redress after businesses fail to protect them from scams. This should include a single door for the consumer to access external dispute resolution, if internal dispute resolution fails. This will improve the experience for scam victims and may increase scam reporting. More reporting of scams should help disrupt and prevent a greater number of scams as these reports provide businesses with intelligence that they should be required to act upon and share with other businesses in the scam ecosystem. It should not be up to the scam victim to navigate the complicated web of businesses involved in the scam ecosystem, especially during what is a stressful and traumatic time. There is potential for it to be very difficult for a scam victim to know which business in which sector had failed to prevent the scam. A simplified pathway addresses this issue and provides a clear first step for consumers.

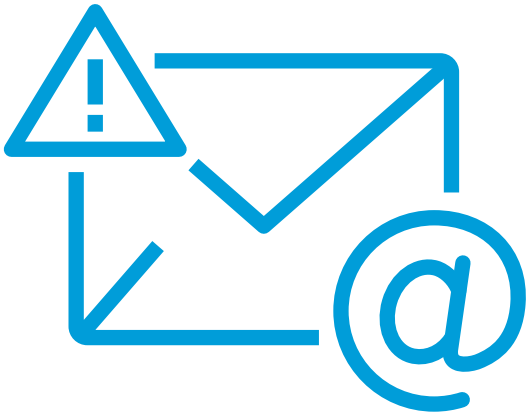
This pathway should also include appropriate support for scam victims. Being scammed can be confusing, traumatic and stressful and the systems put in place should reflect this. Aspects of support could include dedicated, trained staff on the frontline of scam support and regularly updating the consumer on the process of their case.

METHODOLOGY

Passing the buck: how businesses leave scam victims feeling alone and ashamed is based on a survey of 280 Australians that have either themselves been scammed or a family member been scammed involving a bank transfer or debit card, in the last 5 years. The sample includes a spread of people aged 18 years and over, located Australia wide, in each state and territory across metropolitan and regional areas. Fieldwork was conducted from the 19th of October until the 13th of November 2023.

Sample demographics

The sample is spread across all Australian States and Territories, including those living in metropolitan and regional areas. Respondents are spread across all age ranges over 18 with slightly more women than men.



Endnotes

1 Australian Competition and Consumer Commission, 'Targeting scams: report of the ACCC on scams activity 2023' April 2024 https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2023

2 Australian Bureau of Statistics, "Personal Fraud: 2022-23 financial year' March 2024 https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2022-23

3 CHOICE Consumer Pulse June 2023 is based on a survey of 1,087 Australian households. Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was conducted from 7th to 22nd of June 27, 2023

4 Australian Securities and Investments Commission, 'REP 761 Scam prevention, detection and response by the four major banks' April 2023 https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-761-scam-prevention-detection-and-response-by-the-four-major-banks/ p.20

5 Which? UK, 'The Psychology of Scams: Understanding why consumers fall for APP scams' March 2023 https://www.which.co.uk/policy-and-insight/article/the-psychology-of-scams-aizJj8F0E4rY#executive-summary

6 Australian Competition and Consumer Commission, 'Targeting scams: report of the ACCC on scams activity 2023' April 2024 https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2023

7 CHOICE Consumer Pulse June 2023 is based on a survey of 1,087 Australian households. Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was conducted from 7th to 22nd of June 27, 2023

8 Australian Competition and Consumer Commission, 'Targeting scams: report of the ACCC on scams activity 2023' April 2024, p. 14 https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2023

9 Australian Competition and Consumer Commission, 'National Anti-Scam Centre quarterly update March 2024' March 2024, https://www.accc.gov.au/about-us/publications/serial-publications/national-anti-scam-centre-quarterly-update/national-anti-scam-centre-quarterly-update-march-2024

10 Australian Competition and Consumer Commission, 'National Anti-Scam Centre quarterly update March 2024' March 2024, https://www.accc.gov.au/about-us/publications/serial-publications/national-anti-scam-centre-quarterly-update/national-anti-scam-centre-quarterly-update-march-2024

11 CHOICE, 'Scam ads rampant on popular social platforms' September 2023, https://www.choice.com.au/shopping/online-shopping/buying-online/articles/scam-ads-on-facebook-google-instagram

12 Meta, 'Meta Business Help Centre: Confirm your identity to run ads about social issues, elections or politics' https://en-gb.facebook.com/business/help/2992964394067299?id=288762101909005

13 ABC, 'Facebook Marketplace has become the home of scammers. The problem may be getting worse' March 2024, https://www.abc.net.au/news/science/2024-03-01/facebook-marketplace-has-become-the-home-of-scammers/103521536

14 Australian Securities and Investments Commission, 'REP 761 Scam prevention, detection and response by the four major banks' April 2023 https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-761-scam-prevention-detection-and-response-by-the-four-major-banks

15 Australian Securities and Investments Commission, 'REP 761 Scam prevention, detection and response by the four major banks' April 2023 https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-761-scam-prevention-detection-and-response-by-the-four-major-banks

16 Reuters, 'UK's payments regulator lays down mandatory reimbursements in APP fraud victims' June 2023, https://www.reuters.com/world/uk/uks-payments-regulator-lays-down-new-norms-tackle-fraud-2023-06-07/

17 Consumer Action Legal Centre, 'Australian scam victims left behind as UK puts responsibility on banks to reimburse customers' June 2023 https://consumeraction.org.au/australian-scam-victims-left-behind-as-uk-puts-responsibility-on-banks-to-reimburse-customers

18 Beehive.govt.nz, 'Government supports safer digital transactions' March 2024 https://www.beehive.govt.nz/release/government-supports-safer-digital-transactions

19 European Commission, 'Payment services: revised rules to improve consumer protection and competition in electronic payments' June 2023 https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3544

CHOICE