



ASIC
Australian Securities &
Investments Commission

Anti-scam practices of banks outside the four major banks

Report 790 | August 2024

About this report

This is the analysis of our review of the current scam related activities of 15 of Australia's authorised deposit-taking institutions (ADIs), referred to as 'reviewed banks' for the purposes of this report.

From our findings about existing and emerging bank practices in preventing, detecting and responding to scams, we have provided observations for all banks to consider, to minimise the impact of scams on their customers.

Contents

Executive summary	2
Key findings	7
Appendix 1: Snapshot of findings against REP 761	20
Appendix 2: Accessible data points	24
Appendix 3: Review methodology and definitions	25
Appendix 4: Participating entities	27
Key terms, data measures and related information	28

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents: consultation papers, regulatory guides, information sheets and reports.

Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations. Examples in this report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Executive summary

Scams continue to have a devastating impact on Australians, with the ACCC reporting consumer losses of \$2.74 billion to scams in 2023. While ACCC data suggest overall scam losses are decreasing despite increased scam reports, continued efforts are required across industry, regulators and government to ensure this trend continues.

Note: See [Targeting scams: Report of the ACCC on scams activity 2023](#), 28 April 2024.

In April 2023, ASIC released Report 761 *Scam prevention, detection and response by the four major banks* (referred to as [REP 761](#) or 'initial report'), which found that while the four major banks recognised the significant harm caused by scams, their approach to scams strategy and governance was less mature than expected.

Recognising the critical role that all banks have in combatting scams, ASIC has now reviewed the scam prevention, detection and response activities (also referred to as 'anti-scam practices') of 15 banks outside of the four major banks. The data we reviewed gives us point of time information as at 30 June 2023. We recognise there have been significant developments in the anti-scam infrastructure since that time, including the establishment of the National Anti-Scam Centre.

Of the 15 banks, six were included in 'Stream 1' and subjected to in-depth investigations. The balance were grouped as 'Stream 2' and given lighter touch reviews (see [Review methodology](#)). We also gathered updated data from the four major banks to understand outcomes since the initial report (see [Update on the four major banks](#)).

We encourage all banks and financial service businesses to consider the findings in this report in conjunction with our initial report, and to take steps to advance their scam prevention, detection and response activities.

Key data findings

The summary below describes the key observations from the data we collected about the impacts of scams on customers of the reviewed banks during the 2022–23 financial year. For definitions of measures in this table, see [Data measures](#).

Note: Not all reviewed banks are included in the data below (see [Deficiencies in data reporting capabilities](#) and [Review methodology](#)).



\$232m

in total scam transactions made by customers.

Note: These were payments made by customers in total, including those that were subsequently detected and stopped and recovered.



96%

of total scam losses were born by reviewed bank customers

Note: Scam losses are total scam transactions less amounts detected and stopped and/or recovered.



19%

of these transactions by value were detected and stopped.

Note: Detected and stopped excludes other scams that were prevented by the bank prior to the customer performing the transactions.



2%

was the share of scam losses reimbursed and/or compensated by the reviewed banks if the customer did not complain. That share increased to 7% where the customer complained.

20%

of funds transferred were recovered from the receiving banks/financial institutions.

Our observations

Approach to scam detection, prevention and response was immature

Given the findings in ASIC's initial report and the national focus on scams, we found the scam detection, prevention and response practices of the reviewed banks to be less mature than we expected.

Apart from education initiatives, most had not fully implemented the key scam detection, prevention and response activities that were discussed in our initial report. In particular, we found that:

- › **Governance and reporting tended to be fraud focussed.** Only five of the reviewed banks had implemented a scams strategy, with only one strategy fully implemented. Of the banks with strategies, most did not have timelines to implement initiatives or measurable targets to monitor progress against the strategy.
- › **Capabilities to hold or delay potential scam payments were inconsistent across payment channels.** A significant number of reviewed banks did not have payment hold capabilities and the majority had not fully implemented monitor and stop capabilities across all payment channels.
- › **Lack of protection against brand misuse across all telecommunication channels.** Only one of the reviewed banks had fully implemented controls to minimise misuse of its telephone numbers and SMS alpha tags to prevent impersonation scams.
- › **Poor customer experiences due to lack of resourcing and customer focus.** Of the reviewed banks in Stream 1, where we examined underlying policies and procedures, none had end-to-end coverage of the customer scam journey, which lead to poor customer

outcomes as noted below. The reviewed banks did not always consider the likely distressed state and vulnerability of the scammed customer and scam reports were frequently mishandled. This led to delays – in part due to resourcing constraints, financial loss to the customer, unclear and confusing communication, and failure to identify and respond to scam victims who were experiencing vulnerability.

- › **Adoption of inconsistent and narrow approaches when considering liability.** Many reviewed banks lacked a bank-wide approach to determining liability for scam losses resulting in inconsistent outcomes for customers. In addition, policies did not always consider all relevant factors for determining liability.

The data above and our findings below highlight the need for all banks to ensure that scam prevention, detection and response is one of their highest priorities.

It was clear that the reviewed banks had started or accelerated initiatives to combat scams during the 2023 calendar year (in some cases using ASIC's observations in the initial report as a benchmark). This work appears to have had a positive impact on scam losses reported, which fell by 15 percentage points – as a share of the total value of scam transactions made by customers – down from 77% in the first half of the reviewed year, to 62% in the second half.

Variations in anti-scam practices and data outcomes

We also found significant variability in the maturity of the reviewed banks' anti-scam practices, with some quite advanced and close to the level of maturity seen in the four major banks, while others were significantly less developed. There were also a wide range of data outcomes across the reviewed banks.

We found that:

- › **Oversight and investment drive action on scams** – For the reviewed banks in Stream 1 where we analysed copies of internal reporting, better practices tended to correspond with a ‘tone from the top’ that encouraged investment in anti-scam practices. For these banks, the size and resources of the bank were less of a contributing factor to how the organisation managed scams than management’s level of engagement with scam prevention.
- › **Progress is possible regardless of resources** – Both the actions taken by the reviewed banks and the data suggest that the findings of the initial report can be implemented regardless of scale. This is in part due to a smaller bank’s ability to rely on third parties where necessary.
- › **Data issues increased variability** – Deficiencies and limitations in data reporting capabilities, along with a lack of agreed definitions led to data quality issues across most of the reviewed banks. While we have worked to validate the data provided to the extent possible, these issues likely contributed to the variability in data outcomes. It is important that all banks have high-quality data collection and reporting capabilities so that senior management can be provided with the information they need to assess the impact of scams on their customers and the bank’s ability to respond.

Ongoing action required to combat scams

All banks and financial service businesses, regardless of size and scale, should assess their anti-scam practices against the findings of the initial report ([REP 761](#)), which outlines a set of baseline measures covering scam governance, prevention, detection and response.

All banks and financial service businesses need to act swiftly and make further improvements to address the ever-evolving nature and sophistication of scams, as well as the developing regulatory landscape. For example, smaller banks and financial service businesses could consider leveraging industry-level initiatives to improve their ability to recover and return funds to scammed customers.

Recent activity in the scams eco-system

The scams landscape has experienced rapid change since REP 761 was published in April 2023.

While there is still work to be done, the four major banks have made progress in implementing the findings of our initial report. For example, they have developed scams strategies and implemented greater friction capabilities. On average, their ability to detect and stop scams has improved, with the share of scam transactions detected and stopped increasing from 13% in the 2021–22 financial year to 24% in the nine months to March 2024.

The increasing recognition of the impact of scams on consumers and the economy has resulted in greater focus by both industry and government in combatting scams.

In addition to the Australian Government’s proposed [Scams Code Framework](#), the initiatives to improve anti-scam practices include:

- › launch of the [National Anti-Scam Centre \(NASC\)](#)
- › the Australian Communications and Media Authority’s (ACMA) [implementation of SMS sender ID registry](#), and
- › the Australian Banking Association (ABA) and Customer Owned Banking Association’s (COBA) [Scam-Safe Accord](#).

ASIC's actions on scams and our next steps

This review is part of ASIC's broader work on reducing the financial and emotional impact of scams on consumers.

We have:

- › executed targeted communication campaigns including to educate and warn customers about scam activity in the banking sector
- › published a new [investor alert list](#) for consumers to check whether an entity they are considering investing in could be a scam
- › actioned the [takedown of scam websites](#) in partnership with the NASC, and
- › supported the development of whole-of-government policy initiatives, such as the Scams Code Framework.

Disrupting investment scams remains a key priority for ASIC. Following this report, we will:

- › continue to engage with the four major banks about their anti-scam practices and their development of initiatives to combat scams, as part of ASIC's ongoing programmatic supervision of these banks
- › monitor the progress of work by the reviewed banks in response to this report and broader industry activities, and
- › continue to review the scam prevention, detection and response activities of superannuation trustees.

Key findings

Immature approach to scam prevention, detection and response





Our review found:

- › overall a fairly nascent approach to the implementation of scams strategies and low maturity of governance across the reviewed banks, with a fair degree of variability across the group
- › inconsistent and narrow approaches to determining liability for scam losses, and
- › a lack of support for scam victims.

Prior to 2023, few of the reviewed banks had taken steps to address and respond to the specific risks and harms posed by scams. Instead, they incorporated scams response into their broader fraud prevention and response processes. This resulted in practices that were not always fit for purpose and did not reflect the unique nature of scams.

We provide, opposite, a set of foundational anti-scam practices that banks and other financial service businesses should have in place. Further detail of these practices is included in the initial report.

All banks, regardless of size and scale, should assess their anti-scam practices against these baseline measures. They should also consider making further enhancements to their practices based on trends in the broader scam environment and any requirements of the upcoming [Scams Code Framework](#).

Scam response priority areas		
	Scams strategy, governance and reporting	Effective frameworks guide and provide oversight on anti-scam practices and initiatives to respond to developments and emerging threats in the scam environment.
	Preventing, detecting, and stopping scams	Initiatives such as customer education, the introduction of friction across all payment types and channels, and protecting brand assets from fraudulent misuse helps customers avoid significant losses.
	Responding to scams and scam victims	Appropriate and timely responses to scams, including initiating funds recovery, communicating with customers, and preventing further scams on the customer's account, can help reduce further customer distress and improve the likelihood of recovery.
	Liability, reimbursement and compensation	Providing fair and consistent outcomes means considering all sources of liability when determining liability, reimbursement and compensation for scams.

For each of the priority areas, our snapshot observations for the reviewed banks are detailed below. See [Appendix 1](#) for more about the findings for the reviewed banks against the initial report's observations.



Scams strategy, governance and reporting

- › Only five of the reviewed banks had an organisation-wide strategy that included scams at the time of our review. We expected more would have implemented a strategy by that stage, given the devastating impact and quickly evolving nature of scams.
- › We reviewed internal reporting for the banks in Stream 1 and saw only two had detailed regular reporting on scam-specific metrics. Among those, only one included a full suite of metrics on customer experience.
- › Only one of the reviewed banks had completed an end-to-end review of their scam practices. While some performed a review on elements of their scam process, they did not cover the full organisation-wide response to scams or were combined with fraud practices. Further, only two of the reviewed banks had plans to conduct an end-to-end scams review.
- › For most of the reviewed banks, significant deficiencies were observed in their collection of data covering the customer's end-to-end scam experience (see [Deficiencies in data reporting capabilities](#) for further detail).

Banks and financial service businesses should consider opportunities for immediate improvement where existing resources and processes can be leveraged for combatting scams. They should also identify areas requiring further investment, such as by reviewing the operating effectiveness of anti-scam initiatives or assessing and improving the quality of data that is used for reporting.



Preventing, detecting and stopping scams

- › All of the reviewed banks had systems and controls in place to monitor and stop scam transactions on at least some payment channels. Only two had hold capabilities across all payment channels. A further seven had some level of hold capability on some payment channels.
- › The reviewed banks reported they were able to detect and stop approximately 19% of scam transactions made by customers by value and recovered 20% of funds transferred to receiving banks or financial institutions. However, outcomes varied significantly across the entities.
- › While all of the reviewed banks provided some level of customer education about scams, investment in and quality of campaigns varied across the group. Only a small number had executed even limited campaigns targeted at specific at-risk customer cohorts. Further, we saw almost no attempts to measure the impact of educational activities on customer behaviour.



Responding to scams and scam victims

- › None of the reviewed banks in Stream 1 had end-to-end policies and procedures dedicated to responding to scam victims.
- › Their procedures were at times outdated and had gaps in key areas such as the triage of scam alerts, the steps required by frontline staff to identify and respond to scams, and the templates and timeframes used for customer communications.
- › Four of the six banks in Stream 1 reported case backlogs and long call-wait times for customers during the review period. There were significant delays to resolutions, with the average case involving

customer loss resolved in 42 days (with a median of 20 days) and a concerning 15% of cases taking more than 90 days to resolve.

- › While the recovery of funds was not a focus of our analysis, one driver of long case times was banks that receive scam funds (receiving banks) failing to respond in a timely manner to recovery requests from the sending banks. We saw examples of wait times of up to three months to a year for the return of funds and responses to recovery requests, resulting in significant customer distress.

Case study 1: Delays due to inaction of receiving banks

A scammed customer from one of the reviewed banks transferred \$50,000 in scam funds to two accounts at two different financial institutions.

The bank reported these transactions to both receiving banks on the same day as the transaction occurred. Despite this, one receiving bank never responded, even though there were regular follow-ups by the bank during an 11-month period. The second receiving bank responded after two weeks, stating that they recovered a minimal amount, which took almost a full year to be refunded.

The extended delay was unacceptable for the customer and drained resources at the reviewed bank.

Further examples of issues in responding to scammed customers by the reviewed banks can be found below (see [Poor customer experiences](#)).



Liability, reimbursement, and compensation

- › Customers of the reviewed banks bore almost all the financial burden of scam losses, at 96%. The overall share of scam loss reimbursed and/or compensated across the group was 4%, compared to the four major banks' 7% during the 2022–23 financial year, though as discussed below, the major banks' figure was driven by one major bank.
- › At least some reimbursement and/or compensation was paid to scammed customers in around 16% of the cases when there was a scam loss.
- › Only 8% of the reviewed banks' scam victims made IDR complaints.
- › Scam victims who complained to the reviewed banks were more likely to receive some form of reimbursement, with the overall share of scam loss reimbursed and/or compensated at 7% for customers who complained, compared to a share of 2% for those who did not submit a complaint. This follows a similar trend to that observed in the four major banks in our initial report.
- › Three of the reviewed banks in Stream 1 lacked an organisation-wide policy for determining liability, and where appropriate, reimbursement and/or compensation.
- › Liability decisions were largely guided by the ePayments Code across the reviewed banks. However, as scam transactions are generally authorised by the customer, they are not covered under the Code's liability principles. We did observe some consideration of other factors, including the level of customer vulnerability and errors made by the reviewed banks in their scam responses. However, policies and procedures would benefit from further exploration of and guidance on all relevant factors needing consideration when determining liability, reimbursement and/or compensation as discussed in the initial report.

Case study 2: Errors identified only after complaint lodged

One of the reviewed bank's customers was the victim of an impersonation scam where they were contacted by someone pretending to work for that bank. Following the scam call, at the request of the scammer, the customer phoned the bank to get help setting up multi-factor authentication. Soon after, the customer was scammed approximately \$20,000 over several transactions. One of these transactions was detected by the bank, which validated with the customer that these were scams.

It was not until the customer complained to AFCA, and four months after the scam occurred, that the bank investigated the customer's call regarding multi-factor authentication. With new intelligence, the investigation found that 'red flags' had been missed and the initial contact with the customer provided an opportunity for the call centre representative to detect the customer had been coached by the scammer and therefore prevent the scam from occurring.

The bank reimbursed the balance of funds that were not able to be recovered from the other financial institution.

Significant differences in findings across the banks

Our review identified material differences in the maturity level of anti-scam practices across the reviewed banks. In addition, key data outcomes varied across entities.

Top-down influence

Through our in-depth examination of the reviewed banks in Stream 1, we observed that a significant contributor to their maturity was their 'tone from the top' or the degree of management's focus on responding to scams.

Generally, the higher the levels of board and senior management involvement and investment in scam prevention, the greater the quality of scam detection and response capabilities, and the faster the speed of implementing initiatives in response to changes in the scam environment.

Example: Reducing consumer harm through tone from the top

Two of the reviewed banks in Stream 1 began investing in improving scam detection systems, customer care, and experience for victims of scams at an earlier stage than other entities in the sample. Overall, both had better quality governance, reporting, processes and procedures. Generally, they also reported fewer concerning case studies and had more favourable data outcomes than others in the group.

We noted that for both banks, their senior management and boards had a strong willingness to invest in detecting and stopping scams, and set ambitious anti-scam targets. They also had a keen focus on reducing customer harm.

One bank was in part driven to act in response to an increase in impersonation scams impacting their customers. This example highlights the importance of good governance and a willingness to act to limit customer harm.

Outcomes are independent of bank size

In general, across the reviewed banks, our analysis of policies and practices, as well as the data, showed that scale and size did not limit their ability to respond to the findings of the initial report. This is partly due to a smaller entity's ability to outsource to third parties.

For example, we saw the widespread ability of the reviewed banks to apply the findings of the initial report:

- › Most had implemented or were planning to implement stop and hold capabilities for payments, such as blocking or preventing potential scam transactions from proceeding – generally in-house for the larger banks, and outsourced to third-party payment services providers for the smaller.
- › Nine had in place, or were in talks with telecommunication providers, to place their phone number on 'do not originate' (DNO) lists and/or block the use of their alpha tags, which reduces the ability of scammers to make calls or send text messages that impersonate a bank's name or brand, respectively.
- › Generally, the reviewed banks were leveraging existing fraud detection systems and processes to target scams more specifically.

Example: Use of existing fraud detection systems

One of the reviewed banks reported a significant improvement in its ability to detect and stop scams over the review period. It partially attributed this improvement to the creation of a set of scam-focused questions, which are raised when the existing fraud detection system identifies and alerts a transaction.

Further, in terms of data outcomes, some smaller banks in the group closely matched or even outperformed some larger ones on key metrics. This suggests that the scale and size of banks does not generally hinder the development and implementation of anti-scam initiatives.

Given this finding, we encourage all banks and financial service businesses, regardless of size and scale, to consider the recommendations outlined in the initial report.

While some initiatives may be difficult for smaller entities to either develop or implement on their own, there is opportunity to rely on industry-led initiatives such as the ABA and COBA's upcoming confirmation of payee solution, or the new anti-scam measures pioneered and tested by the larger banks.

Deficiencies in data reporting capabilities

We noted significant gaps and varying capabilities in the collection and reporting of data on scams by the reviewed banks. In addition, there was a clear lack of agreed definitions across the sample, including those related to the types and size of scams recorded. For instance, while some entities recorded goods and services scams as a type of scam, others excluded them from their definitions.

These limitations likely contributed to a significant degree of variability in data outcomes. Through our data collection and validation processes, we have worked to improve comparability of data points where possible – this included providing the same [definition of scams](#) to each of the reviewed banks.

Addressing gaps in data capabilities is critical for effective internal reporting to management and boards, as well as accurately measuring the effectiveness of scam strategies.

We did observe improvements in the availability of data from 1 July 2022 to 30 June 2023 compared to 1 July 2021 to 30 June 2022, and we encourage all banks and financial service businesses to review and uplift their scam data processes and capabilities.

Example: Poor data quality

Given their significant contribution to the overall sample, two of the larger reviewed banks with poorer data quality required extensive follow-up engagement by ASIC to resolve comparability issues.

For these, we identified significant issues in the recording of key data points, such as scam amounts stopped, recovered, reimbursed and time taken to close a scam case. These problems stemmed from deficiencies in the data collection process and inaccurate or differing definitions.

Poor customer experiences

Further case studies from the reviewed banks in Stream 1 reveal some particularly poor customer experiences, such as difficult-to-navigate investigation processes that result in further harm to scam victims.

It is vital that systems, processes and procedures account for a customer's likely distress in not only facing the loss of significant amounts of money, but also in dealing with the non-financial harms of having been tricked or emotionally manipulated by scammers. We encourage all banks and financial service businesses to:

- › review their scams reporting to ensure it reflects customer experiences and the unique characteristics of scams, and

- › review training, policies, procedures, and governance structures to ensure scammed customers are treated in a fair, consistent and timely manner and are not impacted by fluctuating levels of scam cases reported by customers.

Some particularly concerning examples of poor customer experiences we saw are outlined below.

Poor responses by frontline staff to scam alerts

The case studies highlight examples where staff missed scam red flags or did not properly escalate cases when identified, resulting in avoidable financial loss and increased distress to customers. Only two of the six reviewed banks in Stream 1 had policies and procedures for frontline staff that covered the key areas of identifying and responding to scams, supporting scammed customers and caring for customers experiencing vulnerability.

Case study 3a: Issues in frontline staff's handling of scam reports

A customer of one of the reviewed banks called their contact centre after accounts with other financial institutions had been compromised. As there was no recent activity on the account, the staff member only added a security word to the customer's account. However, they failed to check for scheduled payments and did not escalate the matter to the relevant scams team in a timely manner to ensure the account was monitored. A few days later, scam transactions totalling \$8,700 were made from the account, which were only detected after being identified by another bank who received the funds. As a result, the bank reimbursed the customer in full.

Case study 3b: Issues in frontline staff's handling of scam reports

A customer service officer at another reviewed bank's branch did not complete a key notification report when submitting a request to recall funds. As a result, the case was not actioned by the fraud team, and fraud reports were only submitted to the other financial institution after the customer lodged a complaint, almost three months after reporting the scam. Due to the frontline staffer's error, the customer was subsequently reimbursed in full.

Multiple staff handoff points for customers reporting scams

We saw examples of reviewed banks splitting their customer journey across a range of teams, such as customer services, payment tracing, recall, and investigation, with some of these functions further split for different payment types (i.e. separate teams for credit card and other scams).

Our review showed that the number of handoffs between these teams presented quite complex systems for customers to navigate. There was a lack of clarity about who to contact and who they were speaking with when contact was made. This resulted in delays in case resolution, inconsistencies in handling scam reports, miscommunications with customers as well as between internal teams, and ultimately poor and frustrating customer experiences.

Case study 4: Complex and poorly designed customer journeys

A customer from one of the reviewed banks lost \$28,500 to a scam. This customer had a particularly poor experience:

- › They could not report the scam when it initially occurred because it occurred outside of business hours.
- › They were told by a contact centre staff member that the transaction would be reversed; however, no reversal was made (the contact centre staff was being guided by a member of the fraud team).
- › Throughout their scams journey, the customer had to contact their bank at least 11 times, engaging with multiple staff from the contact centre, fraud, and complaint teams.
- › An investigation into the transaction was only started by the fraud team when the customer submitted a complaint two months after the scam transaction.
- › While the investigation was still on foot, the customer received an outcome letter stating their bank would not refund the customer and that the customer was fully liable.
- › Three weeks after receiving the initial outcome letter and over four months after the original scam transaction, a full reimbursement was made to the customer as a result of a compliance review that found the bank had made an error and could have prevented the loss of the customer's funds.

It is important that entities consider the end-to-end customer journey, including appropriate contact points, to reduce negative customer experiences.

Poor communication with scam victims

Examples of poor bank staff-customer communication in case studies we reviewed included:

- › giving customers inaccurate and unclear information,
- › failing to set realistic expectations
- › not proactively updating customers on case progress
- › lacking empathy in written communications, and
- › not following processes and procedures during customer interactions.

In one case study, the scammed customer had at least 29 interactions with their bank over the span of 14 months ... and [the bank] incorrectly overstated the amount of funds recovered by \$4,800.

Case study 5: Poor communication with scam victims

- › In one case study, the scammed customer had at least 29 interactions with their bank over the span of 14 months, including having to initiate contact to ask for updates on their case, and to clarify text messages from the bank about the outcome of the recovery process. The bank's customer service team also failed to return calls after promising to do so, and incorrectly overstated the amount of funds recovered by \$4,800.
- › In the case study above and one other case study submitted by the same reviewed bank, the bank sent the scam victims a text message with the outcome of their recovery process. The texts provided limited context, only stating that recovery had been unsuccessful or partially successful. Each of the affected customers immediately called their bank to seek further details. The abrupt nature of receiving these alerts by texts, which deliver potentially devastating news, can cause significant distress to customers, and the messages were not designed with the customer's situation in mind.

Limited focus on customers experiencing vulnerability

Policies and procedures for responding to scam victims are important to help staff provide suitable and consistent after-care arrangements given the psychological distress caused by scam events.

Generally, we found that:

- › while the reviewed banks had general guidance on how to identify and support vulnerable customers, there was limited discussion of or guidance on this topic in their scam-specific procedures, and
- › in case studies provided by the reviewed banks, there were examples where frontline staff and scams teams failed to identify vulnerability, or appropriately refer customers to specialists when vulnerability was identified.

While the reviewed banks had general guidance on how to identify and support vulnerable customers, there was limited discussion of this topic in their scam-specific procedures.

Case study 6: Vulnerability identification

One of the reviewed bank's customers fell victim to a phone scam in which the scammer persuaded them to share their online banking details and purchase gift cards, all under the pretence of securing the customer's funds.

Two weeks later, after they learned that at least some of their loss would not be able to be recovered, the customer lodged an IDR complaint with their bank.

It was only during the first call with an IDR specialist a week later that it was identified that the customer had been a victim of identity fraud six months prior to the phone scam, which likely increased the customers' vulnerability to repeat scams. As a result of this call, the specialist then updated the customer's email address to mitigate the risk it had been compromised. After the customer escalated the complaint to AFCA, the bank made a goodwill payment and reimbursed the unrecovered funds.

Potential indicators of vulnerability should be proactively monitored and reviewed from the outset.

Improvements in bank responses to scam challenges

The issues noted above were generally acknowledged by the reviewed banks as leading to poor customer outcomes and requiring improvement. It was positive to see that the majority of them have either begun or accelerated work specifically focused on combatting scams.

For many of these banks, the impetus for this work was a combination of:

- › the release of [REP 761](#) in April 2023
- › their engagement with the development of the ABA and COBA's [Scam-Safe Accord](#) released in November 2023, and
- › the Government's announcement of an intended [Scams Code Framework](#), also in November 2023.

As mentioned above, two of the reviewed banks responded to the threat of scams earlier than their peers, with the majority only starting or accelerating work during the 2023 calendar year. The nature and scale of scams requires a prompt response and sharp focus by all banks and financial service businesses and we ultimately expected that more action would have been taken sooner.

We found that six of the reviewed banks had proactively completed a self-assessment against the observations made in the initial report, with a further two performing assessments against industry association benchmarks covering similar areas.

Some of the key improvements reported as being implemented or underway at the reviewed banks were:

- › Along with the five with a scam strategy in place, a further six had plans to implement one.

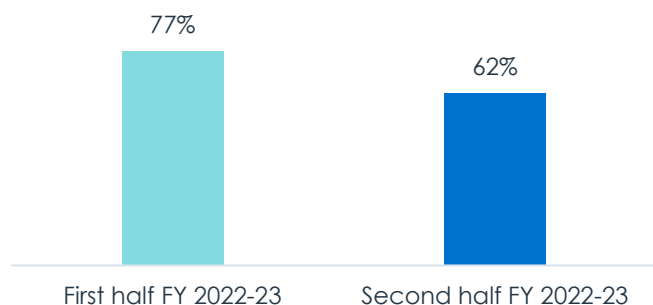
- › Most in Stream 1 had improved, or planned to improve, the quality and content of their internal reporting on scams to their board and senior management.
- › Many had implemented or were considering placing further friction on transactions – including the use of biometrics and the placement of stops or delays on payments to digital currency exchanges.
- › Four in Stream 1 had plans to improve scam-related policies and procedures, such as developing guidance for staff to identify and respond to scams, outlining key timeframes for communications with customers, and integrating processes between different teams involved in their customers' scam journey.
- › Two were considering implementing 24-hour, seven-day monitoring and response capabilities for scam alerts, with a further two already having this in place. This capability can improve customer outcomes and avoid instances where recovery requests are delayed if a customer submits a scam report during the weekend or after hours.
- › Three in Stream 1 had put in place an organisation-wide reimbursement and/or compensation policy, and a further two had plans to implement one.

Reduction in customer losses

Once the reviewed banks started to collectively respond and increase investment in anti-scam capabilities, the data suggests this led to positive customer outcomes, with **scam losses – as a share of scam transactions made by customers – falling by 15 percentage points, from 77% in the first half of the 2022–23 financial year, to 62% in the second half** (see Figure 1).

The improvement was driven by an increase in both the share of scam transactions made by customers which were detected and stopped and/or recovered by the reviewed banks. Only three banks with data available experienced an increase in the share of scam loss over the review period.

Figure 1: Scam loss as a share of scam transactions made by customers during the 2022–23 financial year



Note: See [Appendix 2](#) for the data shown in this figure (accessible version)

Importance of change management

Given the significant pipeline of initiatives, there is a risk that banks will try to implement too much at once and their changes will not have the intended effect. All banks need to ensure that initiatives are fit for purpose, fully embedded, and have the desired impact on customer outcomes.

Example: Governance structures during implementation

One of the reviewed banks had developed a large-scale plan for improving both their scam and fraud responses.

However, a third-party review of the plan, which coincided with its initial establishment phase, identified a number of deficiencies related to change management. These included limited formalised governance and accountability, weaknesses in risk management, and a lack of coordination and consultation with key stakeholders, leading to challenges and inefficiencies – including in implementation.

This bank is taking a number of steps to address the findings, including the establishment of an executive-level oversight committee to coordinate an organisation-wide approach and regularly monitor the progress of initiatives.

We also saw the potential for improvement in some initiatives that had already been implemented, for example:

- › The four examples of anti-scam strategies provided to us by the reviewed banks in Stream 1 differed in quality. Two strategies did not contain timelines to implement initiatives and two had limited examples of measurable scam-specific targets to monitor progress against the strategy.
- › While many of the reviewed banks had completed partial reviews which focused on specific aspects of the scam process or more broadly on fraud, we observed very few examples of completed or planned end-to-end scam reviews.
- › The review of organisation-wide policies for determining liability highlighted the need to develop more in-depth guidance on

different scam scenarios and how they should be considered by staff.

- › We saw limited focus from the reviewed banks on enhancing end-to-end policies and procedures that would ensure a focus on the unique and often distressing experiences of scam victims. As all of the reviewed banks continue to implement anti-scam initiatives, we encourage a greater effort to improve customer experience.

Update on the four major banks

We collected updated data from the four major banks for the 2022–23 financial year and from 1 July 2023 to 31 March 2024 (see Table 1; see [Appendix 3](#) for discussion of methodology). It should be noted that there was variability between the outcomes of each of the banks.

The collective value of scam transactions made by major bank customers increased by 63% in the 2022–23 financial year compared to the 2021–2022 financial year, and then fell by around 9% if the value of scam transactions over the nine months to March 2024 is annualised.

The share of scam transactions detected and stopped increased in the 2022–23 financial year by 10 percentage points to 23%, and remained stable in the nine months to March 2024 at 24%. The improvement was primarily attributed to increased friction on transactions made to digital currency exchanges, as well as enhancements to hold and behavioural biometric capabilities in detection systems.

This measure of detected and stopped does not include attempted scam transactions prevented by the major banks prior to a customer performing the transaction. We recognise that the major banks have put in place initiatives such as confirmation of payee and real-time prompts. The major banks have reported that these initiatives have resulted in

significant amounts of attempted scam transactions being prevented (however this data point did not form part of our data collection).

We saw mixed improvement in the share of scam funds transferred to receiving banks or financial institutions which were able to be recovered. While the share fell in the 2022–23 financial year, three of the four major banks had a particularly strong increase in the nine months to March 2024.

The general increase from 4% to 7% in the share of customer financial losses reimbursed by the four major banks during the 2022–23 financial year was driven entirely by one bank, with the other three having a stable or lower share. However, the share fell slightly in the nine months to March 2024 to 6%. All four major banks are in the process of implementing – or have implemented – an organisation-wide approach to determining liability, and where appropriate, reimbursement and/or compensation for victims of scams.

Table 1: Key outcomes for scammed customers of the four major banks

Key measures	2021–22 financial year	2022–23 financial year	Nine months to 31 March 2024
Total scam transactions made by customers	\$845m	\$1.38bn	\$941m
Total number of scammed customers who experienced financial loss	33,700	61,596	68,317
Share of scam transactions detected and stopped by value	13%	23%	24%

Key measures	2021–22 financial year	2022–23 financial year	Nine months to 31 March 2024
Share of scam funds transferred to receiving banks or financial institutions which were able to be recovered	15%	13%	20%
Share of scam loss reimbursed/compensated	4%	7%	6%
Share of scam victims who lodged an IDR complaint	13%	15%	N/A
Share of scam victims who lodged an IDR complaint with reimbursement and/or compensation	36%	41%	N/A

Note 1: Data not requested for the 2023–24 financial year for the share of victims who lodged an internal dispute resolution complaint and share of victims who lodged an IDR complaint with reimbursement.

Note 2: There were some changes in classifications by the major banks since the original data collection which may have minor impacts on trends over time.

Note 3: The share of scam transactions detected and stopped by value does not include other scams that were attempted but prevented by the bank prior to the customer performing the transaction.

Progress on scam initiatives by the four major banks

Though there is still more to be done, we recognise that since ASIC's initial report, the four major banks have been active in preventing scams including by:

- › implementing a number of friction initiatives to prevent attempted scam transactions from proceeding. For example, partnering with a telecommunication provider to help detect scam calls in real time, and asking customers automated questions before they make a payment to help them identify high-risk transactions
- › implementing scam strategies
- › improving the content and quality of reporting to boards and senior management
- › conducting scam education campaigns targeting at-risk customers, and
- › undertaking review of scam programs by internal audit or customer advocates.

Appendix 1: Snapshot of findings against REP 761

As discussed above, there is significant variability in the maturity of anti-scam practices across the reviewed banks. This means that while many of them may have implemented an observation noted in the table below, one may be significantly more advanced than the other(s). We encourage all banks to continually review, refine and fully-embed anti-scam practices.

Table 2: Scams strategy, governance and reporting

Observations of the reviewed banks	Implemented	Partially implemented	Not implemented	Plans to implement/improve	Notes
Bank had an organisation-wide scams strategy	1	4	10	9	'Partially implemented' includes entities who provided us with strategies which did not contain all elements of a strategy outlined in REP 761.
Bank had board and senior management oversight of scams prevention, detection and response activities	6	0	0	3	Information only collected from the six banks in Stream 1.
Bank had regular reporting to board and senior management	6	0	0	3	Information only collected from the six banks in Stream 1. As noted in the report, only two of the banks in 'Implemented' had detailed scams focused reporting.
Bank's reporting to board and senior management included a focus on customer experience and outcomes	1	3	2	4	Information only collected from the six banks in Stream 1.
Bank systems captured and could automatically report on end-to-end scams cases	0	14	0	6	Data collected from 14 banks only.
Bank had conducted an end-to-end scams review in the past three years	1	10	4	2	

Table 3: Preventing scams

Observations of the reviewed banks	Implemented	Partially implemented	Not implemented	Plans to implement/improve	Notes
Bank had scam awareness education activities	15	0	0	9	
Bank monitored and measured the effectiveness of scam awareness education activities	0	0	15	6	As noted in the report, this refers to monitoring and measurement of the impact of education activities on customer behaviour. This does not include monitoring general engagement metrics, such as click-through rates or open rates.
Bank had added scam-prevention friction in the provision of banking services across all channels and networks	0	15	0	6	
Bank had implemented controls to minimise misuse of its telephone numbers and SMS alpha tags	1	7	7	7	

Table 4: Detecting and stopping scams

Observation of the reviewed banks	Implemented	Partially implemented	Not implemented	Plans to implement/improve	Notes
Bank had ability to hold payments in real-time across all payment channels and networks	2	7	6	5	The review noted a wide difference in hold capabilities for entities in the 'partially implemented' categories. There were two entities that had far more advanced capabilities compared to the remainder of the cohort.

Table 5: Responding to scams and scam victims

Observations of the reviewed banks	Implemented	Partially Implemented	Not Implemented	Plans to implement/improve	Notes
Bank had documented end-to-end processes and procedures for responding to a scam and a scam victim	0	6	0	4	Information only collected from the six banks in Stream 1.
Bank's case study practices aligned with scam processes and procedures	0	6	0	5	Information only collected from the six banks in Stream 1. 'Partially implemented' contains banks with their case study practices aligned with some, but not all, of the bank's scam processes and procedures.
Bank had processes and procedures for staff to identify and support customers experiencing vulnerability and case study practices aligned with these processes and procedures.	0	6	0	2	Information only collected from the six banks in Stream 1. 'Partially implemented' contains banks that had processes and procedures or case study practices aligned with these processes and procedures, but not both.

Table 6: Liability, reimbursement and compensation

Observations of the reviewed banks	Implemented	Partially Implemented	Not Implemented	Plans to implement/improve	Notes
Bank had an organisation-wide policy for determining scam loss liability and reimbursement or compensation	3	0	3	3	Information only collected from the six banks in Stream 1.
Bank's policies in relation to scam loss liability outlines all the grounds on which a bank might be liable	0	4	2	0	Information only collected from the six banks in Stream 1. 'Partially implemented' included banks that had outlined some, but not all, of the grounds on which they may be liable for scam loss.

Appendix 2: Accessible data points

Table 7: Data table for Figure 1

Category	Percentage
Scam loss as a share of scam transactions made by customers during the first half of the 2022–23 financial year	77%
Scam loss as a share of scam transactions made by customers during the second half of the 2022–23 financial year	62%

Note: This is the data shown in Figure 1.

Appendix 3: Review methodology and definitions

Review methodology

The 15 reviewed banks in our sample collectively accounted for around 70% of household deposits (\$278 billion) at non-major bank deposit taking institutions as at March 2024, according to APRA's Monthly Banking Statistics.

The sample consists of eight banks with ABA membership, five from COBA, and, while we collectively refer to the sample as 'reviewed banks', two were purchase payment facility providers.

A study in two streams

All of the reviewed banks were required to complete a questionnaire and provide data on scam cases from 1 July 2022 to 30 September 2023.

Six of the reviewed banks were selected for a more detailed review (i.e. the banks in Stream 1), which involved document requests and case studies. We met with the banks in Stream 1 to discuss their submissions in March 2024. The remaining nine were classified under Stream 2.

Data collection

Data points referred to throughout the report only include data from 11 of the reviewed banks. This is because:

- › one bank was unable to provide scams data due to differences in the nature of their operations as a payments provider/facilitator and scam transaction flows
- › the data of a further three banks was excluded due to queries about data quality or lack of comparability, and

- › one entity was excluded from our measures of 'share of scam transactions detected and stopped by value' as well as 'share of scam transactions sent to other financial institutions able to be recovered by value' as it classified some recovery values as detected and stopped.

For the period 1 July 2022 to 30 June 2023, our data collection from the 11 reviewed banks recorded around:

- › 37,500 scam cases
- › \$232 million in total scam transactions made by customers, and
- › 20,300 scam victims with loss.

For the four major banks, we used scam case level data collected for the initial report, and received updated data for the period from 1 July 2022 to 31 March 2024 on an aggregate basis for key scam-related metrics. As discussed in our initial report, the data request to the four major banks did not define a scam transaction and was provided based on internal definitions.

For the cohort of banks in our current review, we provided a scam definition in line with the explanation below. However, as discussed above, while these banks provided data on a best endeavours basis, differences remained in how they defined scams.

The results of this review should be interpreted in light of these limitations and the issues highlighted in the [Deficiencies in data reporting capabilities](#) section.

Definition of scams

Scams are a subset of fraud where people are tricked into providing information or money. For the purposes of the reviewed banks' data collection and case studies, where possible given data limitations, we employed a narrower definition, limiting scams to situations where customers authorised the transaction by either making the transaction or aiding the scammer to make the transaction, including by providing multi-factor authentication passwords.

This is differentiated from the broader definition of scams where the customer provided the scammer with personal information (such as date of birth and address) allowing them to impersonate the customer and conduct the unauthorised transaction.

The narrower definition allowed ASIC to assess how the reviewed banks respond to situations where, in the current environment, the customer is likely to be liable for the transaction under the ePayments Code, as the lack of recourse leaves customers in a vulnerable and difficult position of potentially losing significant amounts of money.

The broader definition of scams highlights the need for an eco-system approach and the important role that other industries, such as telecommunication providers and digital platforms, play in combatting scams, as scams are often initiated through these channels.

Appendix 4: Participating entities

The entities that participated in our review were:

- › AMP Bank Limited
- › Bank Australia Limited
- › Bank of Sydney Ltd
- › Bendigo and Adelaide Bank Limited
- › Beyond Bank Australia Limited
- › Credit Union Australia Ltd
- › Heritage and People's Choice Limited
- › ING Bank (Australia) Limited
- › Macquarie Bank Limited
- › Newcastle Greater Mutual Group Ltd
- › Norfina Limited (trading as Suncorp Bank)
- › PayPal Australia Pty Limited
- › Rabobank Australia Limited
- › Teachers Mutual Bank Limited, and
- › Wise Australia Pty Ltd.

The review also involved the collection of data from the following four major banks:

- › Australia and New Zealand Banking Group Limited
- › Commonwealth Bank of Australia
- › National Australia Bank Limited, and
- › Westpac Banking Corporation.

Key terms, data measures and related information

Key terms

ACCC	Australian Competition and Consumer Commission
AFCX	Australian Financial Crimes Exchange
AFCA	Australian Financial Complaints Authority
alpha tag	A name that appears as the sender in place of a phone number in a short message service (SMS) message
ePayments Code	A voluntary code of practice that regulates electronic payments
DNO (Do Not Originate) list	A database of legitimate entities' inbound telephone numbers reserved for anti-spoofing purposes
IDR	Internal dispute resolution
scam	Type of fraud, usually with the purpose of getting money or information from people using a deceptive scheme or trick
SMS	Short message service
sending bank	The bank of the scam victim (i.e. the bank from which a scam transfer is initiated)

receiving bank or financial institution	The bank or other financial institution that receives scam funds from a scam victim
third party payment services provider	An external entity that provides banks and other payments services providers with access to payment systems such as New Payment Platform (NPP) and international card schemes (e.g. Visa, Mastercard)

Data measures

Scam transactions made by customers	Value of scam transactions made by customers. This excludes other scams that were attempted but prevented by the bank prior to the customer performing the transaction
Scam transactions detected and stopped	The value of scam transactions made by customers intercepted by the sending bank, prior to funds being transferred to the other financial institution. Does not include amounts prevented by a bank prior to the customer performing the transaction
Recovery and/or scam transactions recovered	The value of scam transactions made by customers returned from the recipient's account to the scammed customer after the scam transaction has occurred (including intrabank transactions)
Scam transactions sent to other financial institutions	Scam transactions made by customers less scam transactions detected and stopped

Reimbursement and/or compensation	The value of payments made to the scammed customer by the bank, excluding scam transactions recovered
Scam loss	Scam transactions made by customers less any scam amounts detected and stopped and recoveries of scam proceeds
Share of scam transactions detected and stopped by value	Total value of scam transactions made by customers detected and stopped as a share of total scam transactions made by customers
Share of scam transactions transferred to receiving banks or financial institutions able to be recovered by value	Total value of scam transactions made by customers recovered as a share of total value of scam transactions sent to receiving banks or financial institutions
Share of customer loss reimbursed and/or compensated	Total value of reimbursement/compensation as a share of total scam loss
Share of customer loss reimbursed if a complaint was submitted	Total value of reimbursement/compensation for customers who submitted a complaint as a share of scam loss
Share of scam victims who complained	Total number of scammed customers who lodged any form of complaint (not limited to IDR) as a share of total number of scammed customers
Share of scam victims with an IDR complaint	Total number of scammed customers who lodged an IDR complaint as a share of total number of scammed customers

Share of scam victims with IDR complaint with reimbursement	Total number of scammed customers who received reimbursement/compensation and lodged an IDR complaint as a share of total number of scammed customers
Average case length	Average number of days taken to finalise an investigation of scam incident/s
Total scam transactions made by customers	Total dollar value (\$) of scam transactions made by customers
Reimbursement/compensation rate	See definition of 'share of customer loss reimbursed and/or compensated'
Share of scam loss borne by the customer	Total scam losses less total reimbursement and/or compensation as a share of total scam losses
Scam loss as a share of total scam transactions made by customers	Scam loss as defined above, as a share of total scam transactions made by customers

Related information

Headnotes

banks, complaints, scams.

ASIC documents

[ePayments Code](#)

[Report 761](#) *Scam prevention, detection and response by the four major banks*