ASIC
Australian Securities & Investments Commission

Scam prevention, detection and response by the four major banks

Report 761 | April 2023

About this report

This report is the analysis of our review of the current scam related activities of the four major Australian banks.

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

Contents

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 are increasing in volume and sophistication, causing significant financial and other harm to Australian consumers, including the most vulnerable people in our community.

Between 1 July 2021 and 30 June 2022, more than 31,700 customers of the four major banks collectively lost more than $558 million through scams. This was an increase of 49% in customers and 50% in financial losses compared to the previous 12-month period. During the same period, banks paid approximately $21 million in reimbursement and/or compensation payments to customers who fell victim to a scam.

Banks have a critical role as part of a broader industry ecosystem that includes financial institutions, telecommunications providers, social media platforms and digital platforms, among others, in helping to minimise the impact of scams on the Australian community by:

- preventing and disrupting scammers from misusing banking services to carry out and financially benefit from scams, and
- supporting customers by having effective scam prevention, detection and response activities.

Recognising the important role of banks in scam prevention, detection and response, we conducted a review of the four major banks' activities in these areas. We focused on the major banks with the expectation that they should have the most mature and effective policies, processes and practices in relation to scams.

Our observations

Through our review, we found that:

- bank customers are overwhelmingly the bearer of scam losses, accounting for 96% of total scam losses across the banks
- collectively, the banks detected and stopped a low proportion of scam payments made by their customers (approximately 13% of scam payments)

  Note: This excludes other scams that were attempted but prevented by the bank prior to the customer performing the transaction.
- the reimbursement and/or compensation rate varied but was low across the individual banks, ranging from 2 to 5%
- customers who made a complaint were more likely to receive some form of compensation payment from their bank, compared to customers who did not, and
- across three banks for whom data was available, we observed reimbursement and/or compensation paid in only around 11% of the cases where there was a scam loss.

While the major banks recognise the gravity and significance of the issue, they can and should do more to protect Australians from the financial loss of scams. From our review, we observed the following:

- **The overall approach to scams strategy and governance was highly variable and, overall, less mature than we expected**—only one bank had a documented bank-wide scams strategy; two banks regularly reported customer experiences of scams and their outcomes to senior management; and only one bank had recently conducted an end-to-end review of its scams practices.
- **Banks had inconsistent and narrow approaches to determining liability**—for example, none of the banks had a bank-wide approach to determining liability for scam losses, which meant that a scam victim might get a different outcome depending on which bank they are with and which department of their bank they dealt with when seeking financial reimbursement after falling victim to a scam.
- **Scam victims are not always well supported by their bank**—for example, we observed resourcing issues which meant that for some banks scam cases were not being resolved in a timely manner; process gaps and lack of clarity in processes that caused inconsistent and sometimes poor customer experiences; and gaps in how the banks identified and managed customers experiencing vulnerability.
- **There are gaps and inconsistencies in the abilities of the banks to detect and stop scam payments**—for example, the ability to hold payments in real-time differed between banks, and depended on the specific payment channel and network involved.
- **While there were examples of emerging good practice, overall there was a great deal of variability in the steps being undertaken by the banks to help prevent their customers from becoming the victim of a scam**—for example, some banks were imposing more friction into the payments process than others; some banks had been more successful in working with telecommunications providers to implement measures to minimise misuse of their phone numbers and SMS 'alpha tags'; and some banks had been quicker to adopt new technologies.

This report outlines the findings from our review and highlights some of the initiatives that we saw banks undertaking to minimise the impact of scams on their customers. We encourage all banking and other financial service businesses to consider the findings outlined in this report and take steps to advance their scam prevention, detection and response activities.

Given the evolving nature of scams and the degree of customer harm we have observed, we expect scam prevention, detection and response activities to continue to develop and improve, beyond what is identified in this report.

Background and approach to our review

Background

Scams—a type of fraud where people are tricked into providing information or money—are increasing in their volume and sophistication. Scams cause significant harm to Australians, and their advancing sophistication means all Australians are at risk of falling victim to a scam.

The increase in scam activity over time has been driven by a number of structural factors. Two of these factors are the advances in technology that have improved a scammer's ability to easily and cost-effectively target and contact scam victims; and the move towards digital financial services, which has made it quicker and easier to both send and receive scam payments.

These structural factors, along with consumers' increased digital adoption and isolation during the COVID-19 pandemic, have amplified the importance of effective scam management by all entities across the broader scam ecosystem. This includes, among others, financial institutions, telecommunications providers and digital platforms.

Although this report references actions that banks can take to help prevent customers from becoming the victim of a scam (including through education and warnings), we note that scammers use a range of psychological techniques to manipulate scam victims and overcome those measures. In this context, efforts by all parts of the scam ecosystem to disrupt and prevent scams at their source will take on increased importance.

Our approach to this review

We reviewed the scam prevention, detection and response activities of the four major Australian banks:

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

Between May 2022 and February 2023, we reviewed material supplied by these banks, including their scam related policies, procedures and other information. We analysed their scam data and met with each bank twice to better understand their practices. Our review also included in-depth consideration of two scam case studies for each bank. The results of our analysis of the banks' scam data are presented throughout this report.

What we are doing next

We will be monitoring the actions taken by the four major banks in response to the improvement opportunities identified in this report. In addition, we have commenced a review of the scam prevention, detection and response activities in other parts of the banking industry.

In addition, disrupting investment scams is an ASIC-wide core strategic priority, and this work is part of ASIC's broader work to address the impact of scams on Australians. As part of this work, ASIC is contributing to whole of government initiatives, including the establishment of the National Anti-Scams Centre.

Scams strategy, governance and reporting

Through our review, we identified that the overall approach to scams strategy, governance and reporting at the major banks was highly variable and, overall, less mature than we expected.

The increasing frequency, sophistication and impact of scams makes it important for all banks to have an effective framework to guide and oversee their scam prevention, detection and response activities. A bank's scams framework should include:

- a strategy to address and respond to scams
- appropriate governance arrangements, and
- effective reporting, including on customer experience and outcomes.

Scams strategy

We consider that to minimise the overall impact of scams on their customers, each bank should have a bank-wide scams strategy. A bank-wide strategy can help to ensure there are bank-wide objectives in relation to scams, and clear accountabilities and measures in place to support achievement of those objectives. It can also support decision making throughout the organisation and the deployment of resources to achieve the objectives.

The existence of a bank-wide scams strategy is particularly important when there are a large number and broad range of teams that need to be working effectively together, significant investments are required, and difficult decisions need to be made (some of which will conflict with commercial imperatives) for banks to be effective in preventing, detecting and responding to scams, and minimising the impact of scams on their customers.

We found that only one of the major banks had a documented bank-wide scams strategy. The strategy, approved in 2022, outlines the bank's coordinated approach to reducing the impact of scams.

> **Example: Bank-wide scams strategy**
>
> The bank's scams strategy consisted of several goals, including improving customer outcomes and experiences and reinforcing trust and confidence in the bank. The strategy outlined initiatives to achieve those goals, including: customer education and awareness campaigns; increasing payment friction; improving scam detection capabilities; and improving the effectiveness of scam interventions and scam related customer experience.
>
> The strategy also included measurable success targets for improving scam prevention and detection rates, and improving the customer experience (measured by survey scores) for scam victims. There were also timeframes and accountabilities for the scam initiatives, as well as a governance model for the overall strategy.

One of the other banks did not have a documented bank-wide scams strategy, but did have a scams uplift forum and program, which collectively included most of the key elements of a strategy.

The remaining two banks did not have a bank-wide strategy, however both had them in development. Although lacking a strategy, both of these banks had a range of initiatives planned or underway to improve their approach to scams.

Oversight by boards and senior management

The significant and growing impact of scams on bank customers, and the potential for inadequate scams management to adversely impact trust and confidence in each bank, led us to expect oversight by senior management and the board of each bank in relation to scam prevention, detection and response activities.

We found that there had been reporting relating to scams to the board and/or senior management committees at all of the banks, although the frequency of this reporting varied.

For three of the banks, matters relating to scams were regularly reported at senior governance forums. For two of these banks, although one only recently, scams were a standing agenda item at the board and senior executive committee levels. The focus on scams by the board and senior management at these two banks recognised the rising impact of scams on their customers at the most senior level of the organisation. It also reflected the importance of monitoring the effectiveness of a bank's scam prevention, detection and response activities to protect customers' continued trust and confidence in the bank.

For the remaining bank in our review, matters relating to scams were reported at board and/or senior executive meetings from time to time, as relevant updates arose.

Internal reporting to boards and senior management

To support effective oversight of a bank's scam prevention, detection and response activities, we consider there should be regular reporting to the board and senior management. Reporting should cover a broad range of matters including the scams threat environment, operational efficiency and effectiveness, customer experience and outcomes.

We found that internal reporting on scams to the board and senior management differed significantly across the banks.

Only two banks provided detailed and regular reporting about scams to their board and/or senior management that had a focus on customer experience and outcomes. For one bank, this included customer experience service-level metrics on timeframes related to calls, customer losses and types of scams, and customer complaints. The other bank had recently provided its board and senior management with similar detailed reporting focusing on customer experience and outcomes. This bank had also reported its scam review findings and recommendations (which focused on customer experience and outcomes) to the board and senior management.

For two of the four banks, reporting was largely focused on scam losses, the scam threat environment, and operational efficiency and performance. For one of those banks we saw some operational reporting to other levels of management in the bank covering customer experience and outcomes.

Scam-related data and systems capability

For banks to effectively report on scammed customers' experiences and outcomes, their scams systems need to be implemented to enable analysis of scam cases in an end-to-end manner.

We asked the four major banks for a dataset containing scam related transactional and complaint data for the period 1 July 2020 to 31 August 2022. The request did not define a scam transaction, and instead, this was determined by each bank according to their own internal definition(s). Therefore, any differences in the way banks classify scam transactions may affect the data presented in this report.

While all of the banks provided a response, there were some caveats and limitations to the data. These were generally caused by system or process limitations—for example, the inability to link complaint records to scam cases.

These caveats and limitations were of such a nature to limit the reporting that can be undertaken on the customer experience and outcomes, for example, relating to scam related complaint volumes, timeframes and reimbursements paid. This in turn limits the ability of management to provide oversight of these areas and to drive continuous improvement.

Throughout this report we include the results of our analysis of the scam related data provided by the banks. While we have used our best efforts to analyse this data and provide insights in a consistent way across all the banks, the results should be interpreted having regard to the above limitations.

Ongoing review of scams prevention, detection and response capability and activities

Banks need to undertake regular reviews of their scam prevention, detection and response activities to ensure these activities remain fit for purpose in a rapidly changing threat environment, and are effective and working as intended to support fair customer outcomes.

Only one bank had carried out review activities across its scams prevention, detection and response capability and activities during the past three years. That bank had recently carried out multiple reviews of its scams capability (undertaken by its customer advocate and internal audit functions) and identified continuous improvement opportunities, including relating to improving customer experience. We found that the work of the customer advocate function at this bank in particular had further elevated the attention given to the bank's scam management.

While another of the banks had not undertaken an end-to-end review of its scams capability, it did have an independent consultant review how the bank conducts scam related customer conversations with its customers, and had made improvements. This bank had plans for its internal audit and second-line risk teams to undertake a review of scams and the bank's scams governance framework.

The remaining two banks had plans to conduct an end-to-end review of their scams capability during 2023. In addition, the customer advocate (or equivalent) for these banks are considering or will also be undertaking a scams related review.

Preventing scams

Preventing a customer from becoming the victim of a scam not only avoids the significant financial losses that may be associated with a scam (for both the bank or the customer), but also the significant distress and inconvenience that might otherwise be caused for that customer.

While we saw examples of emerging good practice (including in some of the innovative measures by some banks), overall there was a great deal of variability in the steps being undertaken by the banks to help prevent their customers from becoming the victim of a scam.

Scam prevention activities undertaken by the banks included:

- customer scam awareness and education
- increasing friction when conducting payments to give customers more time and opportunity to identify that a payment may not be legitimate, and
- taking steps to reduce the risk of their brand assets being misused by scammers.

Scam awareness education activities

Banks have a strong understanding of the scam threat environment and of how their customers interact with their services. Banks also often have a strong relationship with their customers, and a deep knowledge of their financial circumstances and banking practices. To help reduce the incidence of scams, banks should apply this knowledge and understanding to educate their customers about scams. Banks should also regularly monitor and measure the effectiveness of their scam awareness and education activities, and use the results from their reviews to inform their approach to future scam awareness and education activities.

We found that all banks were undertaking activities aimed at strengthening scam awareness and their customers' ability to identify them. This included messaging on the front pages of their websites about fraud and scams. These warnings linked to cyber safety landing pages for hubs that provide various information on: how to stay safe online and avoid becoming the victim of a scam; current scam alerts; how to report suspected scams or fraud messages; and how to get assistance.

The banks also provided scam awareness through other channels including: internet and mobile banking alerts; email communications; text messages; commercial radio and print advertising; and social media posts. We also saw that the banks are increasingly undertaking targeted scam awareness messaging, for example to elderly customers, and about scam typologies relevant to specific customers.

> **Example: Scam awareness targeted to elderly customers**
>
> One of the banks has prepared educational material targeted towards customers over the age of 70. This is a cohort the bank has identified as having a higher risk of becoming a scam victim.
>
> This bank has developed a guide to help older people avoid scams and also established a dedicated scams team focused on customers in this age group. The bank reported that, for the period November 2020 to February 2022, its dedicated team had successfully declined

or prevented $32.6 million worth of scam transactions for this customer demographic.

At least one other bank also had plans to send tailored communications to this cohort.

Awareness and education activities are an important part of an overall scams prevention strategy. However, we found there was very limited, or in some cases, no apparent monitoring of the effectiveness of these activities in helping customers to better identify and avoid becoming the victim of a scam.

One of the major banks had plans to test the effect of a campaign on customer behaviour by delivering bespoke scam awareness videos to certain customers and using data to determine whether those who clicked on the video were less likely to be scammed in the future.

One bank advised that they had interviewed scam victims to understand what could have been done to stop these customers from being scammed. They reported that one of the highest response categories for this question was 'increased awareness and education'.

By monitoring scam prevention activities, banks can review their campaign messages against any changes in customer awareness and the number of scam cases. They can also measure the effectiveness of particular types of communication or delivery methods to identify those having the greatest impact on reducing scams.

Friction in the provision of banking services

Historically, high value transactions have usually been conducted through an assisted service channel, such as in a branch or by phone. This gives bank staff the opportunity to identify unusual transactions—such as those consistent with scam typologies—and to make inquiries with the customer before executing the transaction.

Among other benefits, the move to digital payment channels has made it quicker and easier for customers to make payments. However, it has also increased the speed of moving scam proceeds, and reduced the opportunity for banks to identify and intervene in some types of scam transactions.

In this environment, banks should consider the benefits that appropriately designed levels of friction may offer, to allow:

- customers more opportunity to identify that they have been the victim of a scam and enable them to seek recovery of the funds before the funds leave the bank, and
- the bank to make reasonable inquiries with their customer, if the bank is on notice that the transaction may relate to a scam.

Banks should also monitor the effectiveness of any increased friction measures to ensure they are having the intended outcome, and make changes as necessary.

We found that bank staff involvement is still an important scam prevention method for transactions conducted using assisted service channels. For example, one of the banks uses a process where the branch network staff are required to make meaningful inquiries with the customer about certain transactions and types prior to completing them.

This bank reported that it will conduct due diligence on account activity whenever there is an opportunity to intervene. This includes providing warnings to customers about the risk of making those payments and the unlikelihood of recovering the funds if the transaction ends up being a scam.

We also found that banks, in varying ways, are seeking to reintroduce some friction into the digital payment process, particularly for high-risk transactions. This friction allows the customer time to identify that they have been the victim of a scam and to stop the payment. It also allows time to communicate a scam risk to customers—whether electronically or verbally. Some examples observed included:

- all of the banks have introduced delays in payment processing, although the implementation of this varies both across the banks and within, depending on the payment channel and network used. Further, across the banks we saw considerable differences in the scenarios and circumstances in which friction has been added (e.g. some held payments to new payees for a period of time while others did not), and
- one bank has introduced prompts for the customer to review before making a payment that triggers certain risk alerts, such as for first time investments in crypto-currency.

We also found that there are significant differences in the capabilities and ambitions of the banks. One driver of these differences is that adding friction to payments—for example, by delaying payment execution—is inconsistent with the expectations of some customers. The potential for negative customer reaction will serve as a disincentive to some banks implementing those types of measures.

To the extent that increased friction involves new warning messages, prompts or screening questionnaires, there is the potential for customers to experience 'warning fatigue' over time, reducing the effectiveness of this tool. For this reason, the effectiveness of warnings and similar tools should be monitored, and changes made where there is evidence of decreased effectiveness.

Protecting against misuse of a bank's brand and brand assets

The increasing sophistication of scams that use bank branding makes it harder for customers to identify that a communication by email, text or phone is part of a scam. There are some typologies involving a scammer impersonating the customer's bank. For example, phishing is where a scammer generally contacts a customer, including through phone, email or text message, and appears to be from a legitimate business such as a bank.

The purpose of phishing is to trick the victim into providing personal information such as information about themselves or their login, a password or other bank details. The scammer might then use the personal information to socially engineer the victim to cause them to make a payment or install malware onto their device, or the scammer might use information such as the victim's login credentials to make payments from the victim's account.

In this context, banks need to vigilantly monitor for the fraudulent misuse of their brand, and make use of all available measures to protect their brand and brand assets from being misused by scammers.

We found that all of the banks are active in this regard, and seek to prevent their customers from becoming the victim of attacks that misrepresent their brand and brand assets. For example, the banks ask customers to forward suspicious messages to them, and they also work

with domain registrars, telecommunications providers and others to take down phishing websites and disable scammer contact numbers.

One of the more sophisticated scam typologies involves sending text messages where the sender's number appears as the bank's name or brand, using an SMS 'alpha tag'. This means that when a recipient receives the scammer's message it appears in the same thread as past messages received from the bank, making the incoming text message appear more legitimate.

Banks can work with telecommunications providers to block messages with specified alpha tags (e.g. a bank's name) that are not from an approved point of origin. While there are limitations to the effectiveness of these interventions, only two of the four major banks had implemented blocking for at least their most commonly used alpha tag. The other two banks are yet to implement any alpha tag blocking, but had approached the telecommunications providers to discuss the possibility of implementing this prevention measure.

Banks can also work with telecommunications providers to reduce a scammer's ability to make calls that fraudulently appear as though they are coming from a bank's phone number. This is done by placing the bank's number on a 'do not originate' list. We found that only two of the four major banks had implemented this control, while the other two had approached the telecommunication providers regarding implementation of this measure.

ASIC notes that this is one area where it is important for the broader scam ecosystem—including banks and telecommunications providers—to work together to strengthen the response to scams.

Other scam prevention initiatives

The rapidly changing nature and increasing sophistication of scam typologies makes it important for banks to continue to trial and implement a range of innovative ways to prevent customers from becoming victims of a scam.

To address new and emerging scam typologies, banks should consider the range of contributors to scam activity and the changes they can make to how they deliver services. They should also ensure their prevention initiatives remain relevant and fit for purpose.

Scam prevention initiatives across the banks are being developed and deployed at varying extents and paces. Some of these initiatives include:

- in the absence of a system-wide confirmation of payee framework, one bank is implementing functionality to show customers whether the name and account details match the payee. Another bank is implementing a process to hold a payment for four hours if there is a potential account name mis-match, to allow time to notify and enable the customer to review the transfer (these activities aim to reduce business email compromise scams and other payments to the scammer)
- another bank encourages customers to make payments using PayID, which shows the payment recipient's name with the PayID identifier (e.g. a mobile phone number) before the paying customer proceeds with the payment transaction
- at least two banks are replacing as much SMS (text) communication as possible with secure messaging through their banking app, to avoid the issues associated with the misuse of alpha tags, and

› one bank has introduced a feature for customers to verify whether a caller claiming to be from the bank is legitimate, by triggering a security message in the bank's app, for verification (see the example below).

> **Example: Bank preventative initiative—customer verifies details through the bank app during a phone call**
>
> One of the major banks recently introduced a step to better support customers during a phone call by using the bank's app to verify that they are talking to a bank employee.
>
> At the customer's request or otherwise, this scam prevention initiative allows bank staff to trigger a notification to the customer's banking app. Receipt of the alert by the customer confirms that their call is with the bank. The customer's response to the notification before proceeding with the call avoids the need for their personal details to be provided verbally.

Detecting and stopping scams

Banks have a range of data and tools available to try and detect a customer transaction that may relate to a scam. They also have partnerships, including with the Australian Financial Crimes Exchange (AFCX), where they share intelligence on scams. Once suspicious activity is identified, banks can take steps to stop scam transactions from proceeding. For example, the bank can notify and make further inquiries of the customer before completing the transaction.

We found that banks are detecting and stopping a low proportion of scam payments, and that the capability to detect and stop scam transactions varies both across and within banks.

Rate of detection and stoppage

During the period 1 July 2021 to 30 June 2022, a total of $845 million in scam transactions were made by customers across the four major banks. Of this, around $109 million in payments were detected and stopped by the banks (approximately 13% of scam payments).

The proportion of payments detected and stopped by each individual bank varied between five and 18%. There are a range of factors to explain the difference in detection rates, such as differences in data quality or recording, the way that products and services are provided, and the operation of scam and fraud prevention systems.

Note: The total amount of $845 million excludes scams that were attempted but prevented by the bank prior to the customer performing the transaction.

Scam detection and stoppage capabilities

To maximise their ability to detect and stop scam transactions, banks should have capabilities implemented across all payment types and channels that allow them to detect, hold and assess potential scam transactions.

We found that all of the banks have in place transaction monitoring to detect transactions that are consistent with fraud and scam typologies. The banks varied in their approaches to setting detection rules and thresholds, but generally included consideration of the rate of false positives associated with a detection rule, the impact on customer experience (including for those impacted by false positives), and the actual or potential financial loss associated with the fraud or scam. Operational capacity—for example, the ability to respond to scam alerts—was also a major driver in how rules and thresholds were set.

We found that what happens once a transaction is detected as a potential scam differs between banks, and even within banks, depending on the payment channel and network used.

In many cases, a detected potential scam transaction is held in real-time until the bank can make inquiries with the customer about the transaction. However, in some other cases, the bank has no ability to hold a payment in real-time and instead can only reject the payment, or make inquiries after the payment has been sent. By then, it may be too late to recover the funds. This can impact the ability of the bank to stop a scam transaction.

Case studies: Transactions detected by banks

- A bank customer made five payments, totalling more than $70,000, to the same recipient. The first transaction was held for more than 20 hours, and the second for more than 10 hours, to provide an opportunity for the customer to reassess the transactions.
- Another bank's scams system detected and quarantined three payments for eight hours to provide an opportunity for the bank to assess and contact the customer, if required. However, the transactions were not actioned by the bank within an eight-hour period, resulting in the release of the payments.

The banks are also using a range of device analytics and behavioural biometrics capabilities to identify unusual customer activity during transactions. However, the take-up of this functionality differs across the banks and across different payment channels.

We found that the banks regularly monitor and assess the performance and effectiveness of their detection systems and calibrate and refine them accordingly. This includes reviewing undetected customer reported scams to determine any changes required.

Responding to scams and scam victims

When a bank identifies that a customer may have been scammed (or a customer notifies the bank of this), the bank seeks to respond by undertaking actions such as:

- obtaining information about the scam and transaction
- contacting and requesting the other financial institution to freeze funds and seek reversal (where funds are still available)
- providing the customer with details about next steps, including the recovery process, expected timeframes and potential outcomes
- putting the customer in contact with support services
- assessing liability and arranging compensation or reimbursement (see Liability, reimbursement and compensation)
- providing the customer with education on scam awareness to reduce the risk of them being subject to further scams
- if required, re-setting passwords, removing account blocks, reissuing compromised cards, and
- sharing scam related data with the Australian Financial Crimes Exchange (AFCX), law enforcement and other agencies as required.

Responding to a scam in a timely and effective manner can reduce further distress for the customer and help them better manage the situation. It can also improve the likelihood of being able to recover a customer's scammed funds.

We found that there were multiple areas for improvement in how the banks responded to scam victims. These areas relate to resourcing, policies and procedures, and the identification and management of customers experiencing vulnerability.

Resourcing

Banks should ensure they have sufficient resources to enable them to respond to scams in a timely and effective manner. They should also ensure that the skills and experience of staff take into account the unique needs of scam victims.

A lack of adequate resourcing can lead to delays and cause further distress for customers due to them not knowing the progress of their matter. This can also lead to further hardship or inconvenience as the result of delayed outcomes. In addition, delays by either the sending or the receiving bank, as well as the time the customer takes to identify and report the scam, can reduce the likelihood of recovery of funds for scam victims.

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. Across three banks whom data was available, two banks showed increasing scam case backlogs over the year to 30 June 2022. We were advised that some increases were the result of waiting for other financial institutions to respond on recoverability.

As a consequence of the resourcing issues, we saw:

- delays in seeking recovery of funds or in following up fund recall requests with other financial institutions
- delays in responding to financial institutions' requests for the recovery of funds
- increases in scam related call wait times
- delays in communicating with customers or failing to keep them informed of the fund recall response progress, and
- banks without the capacity to review all potential scam transactions that generated a scam detection alert on a timely basis, or at all.

Case study: Bank delay causing poor customer experience

From early to mid-June 2021, a bank customer unknowingly made five payments totalling more than $70,000 to a scammer. In mid-August 2021 the customer contacted their bank with the details. On the day of receiving the information, the scam victim's bank alerted the receiving financial institution that the five transactions were the proceeds of a scam. They asked on behalf of the customer whether the funds were still available for recovery.

More than four months later, in January 2022, the bank contacted the receiving entity to follow up their earlier request. The receiving entity responded four days later to advise that there was nil recovery possible.

On occasion, the Australian Financial Complaints Authority (AFCA) has required the major banks to compensate customers for non-financial loss due to bank delays in making or following up recall requests, and in communicating with customers about scam related complaints.

We observed increases in the number of staff dedicated to scams across all the major banks, with one bank in the process of further increasing their scam related resourcing levels. However, as noted above, these increases were not always aligned with the increase in scams.

Some of the banks recognised that the skillset required for interacting with scam victims is different to dealing with other types of fraud (e.g. victims of unauthorised transactions). Scam victims often require a more intensive case management approach compared to victims of other fraud. Some of the banks also reported that they are increasingly seeking to recruit staff members with the skills and experience to engage effectively and sensitively with scam victims.

Processes and procedures

To support fair and consistent customer outcomes, banks should document their end-to-end internal procedures for responding to a scam or scam victim.

We found that none of the banks had fully documented their end-to-end process for responding to a scam or a scam victim. The scam related processes and procedures that did exist lacked the clarity to support the consistent management of scams. This included in the areas of:

- how scam alerts and cases are prioritised
- timeframes for assessing scam alerts
- scam case management and timeframes

- contacting and responding to other financial institutions
- communications with customers, including when to provide them with progress updates
- dealing with vulnerable customers
- liability, reimbursement and compensation, and
- the scams team's role during the complaints process.

We also found that some processes and procedures required improvement, in particular regarding the banks' written correspondence with customers.

We saw evidence that these weaknesses were in some cases contributing to poor customer experiences at a time of potentially great distress for them. For example:

- for two banks, the letters sent to customers advising that their money could not be recovered lacked an acknowledgement of the impact on the customer, did not include referral to support services or any education about scams
- for two banks, the letters sent to customers advising that their money could not be recovered were not clear about the options and process for the customer to make a complaint
- for one bank, the letter sent to a customer advised that their money could not be recovered, followed later by an email advising, in error, that their money could be recovered
- for one bank, the staff member advised the customer (after lodging a scam related complaint for them) that the complaint team 'will contact you when they contact you', and advised the customer that they didn't know when this would be because they were from a different team, and
- there were multiple instances where the banks did not update their customers within the timeframes advised by the bank.

Case study: Bank's response to scam victim

In May 2022, the bank detected and stopped several scam transactions made by a customer. Through conversation, the bank identified that the customer had made two other scam related payments in the preceding two days, totalling $40,000. That same day, the bank attempted to recover the payments and was advised five days later by the receiving bank that the recovery was unsuccessful. The bank advised the customer on the day they received the information, that the funds could not be recovered.

In July 2022, the same customer raised a complaint about another disputed transaction and in correspondence to the customer about the transaction, the bank mistakenly noted that they were able to recover the $40,000 payments.

The customer subsequently made a complaint, and the bank offered the customer $4,000 in compensation to resolve the complaint and assist in restoring good faith and the customer relationship.

Some of the case studies that we reviewed included parts that were handled well, including with clear, timely and empathetic communications. When this was the case, it appeared to be attributable to the skill and experience of the staff member involved.

All of the banks have in place, or are developing, tools to help staff hold complex conversations with scam victims to prevent staff from further contributing to customer distress, and to help staff meet expected customer conversation standards.

Identification and management of customers experiencing vulnerability

The nature and increasing sophistication of scams means that everyone is at risk of becoming a scam victim. However, there are some bank customers, who will be experiencing a pre-existing vulnerability that places them at greater risk of harm.

Becoming a scam victim may also cause a customer without a pre-existing vulnerability to experience vulnerability due to the emotional distress or the financial impact of the scam, and thus be at greater risk of further harm.

Banks should identify and document their approach to ensure that when responding to a scam they take extra care in dealing with customers who are experiencing vulnerability. Banks should ensure this approach is consistently followed.

We found that despite internal policies and procedures requiring them to do so, banks did not always identify customers experiencing vulnerability as part of their response to a scam, nor did they take extra care in dealing with this cohort.

As part of our review of case studies, we saw examples where the bank had failed to identify that a customer may be experiencing vulnerability, despite signs that this was potentially the case. This is illustrated by the following case study, where the fact that the customer was experiencing vulnerability was only picked up in a later conversation, and only in more detail, after that customer's contact with the bank's complaints team.

Case study: Bank's response to scam victim

In April 2021, the customer reported to their bank that they were the victim of a scam, and had made several payments to a scammer totalling $28,000. The bank's filenote of the conversation focused on how the scam was perpetrated.

On the same day, the bank sent the customer an email that provided links to external websites and noted, among other things, 'there are some very useful websites below which will assist you moving forward', and 'your best defence is to be aware, educate yourself and always use good judgement'.

Almost six weeks after reporting the scam, the customer contacted the bank again. The bank's filenote of that conversation reported that the customer claimed to have ADHD, and as a result, suffered memory lapses.

Shortly after being advised about the nil recovery, the customer lodged a complaint with the bank.

Next, the bank's complaints team contacted the customer to investigate the matter. As part of this discussion, they identified that the customer was a refugee, and had been experiencing depression and anxiety for three years.

In July 2021, the bank offered the customer $17,000 as a one-off goodwill gesture.

At all of the major banks, staff were guided to refer customers experiencing vulnerability to a dedicated customer support team. However, we saw examples of customers experiencing vulnerability, due to age or mental health issues, where the bank did not refer the

customer to that team in accordance with its policies and procedures. The failure to do so, and in the absence of frontline scam staff being trained in vulnerability management, may make it harder for the bank to ensure it takes extra care in dealing with customers experiencing vulnerability.

We found that some of the banks had developed detailed staff guidance for dealing with vulnerable customers, including:

- one major bank had developed a dedicated comprehensive document for staff about customers who are vulnerable to financial abuse, scams or fraud. This document lists signs of customer vulnerability specific to financial abuse, scams or fraud and discusses the use of a scam alert notification (for customers who have been previously impacted by a scam), with a detailed procedure to identify and help vulnerable customers who may have been scammed, and
- at a different major bank, when staff are making inquiries following a scam related transaction alert, they are required to use 'effective' questions to understand whether the customer is vulnerable, or falling victim to an online scam. If the customer is vulnerable and unsure, staff are required to reject or reverse the payment (if the transaction is in scope and able to be rejected). The bank also provides staff with examples of vulnerability warning signs that may put the bank on alert to make reasonable enquiries.

We also found that some of the major banks have commenced, or will be commencing, staff training in the area of vulnerability management.

Liability, reimbursement and compensation

As outlined above, in most cases, a bank is unable to recover funds once they have been transferred to a scammer.

Given this, whether a customer suffers financial loss will often depend on their liability for the transaction and/or the bank's policies in relation to reimbursement and compensation.

We found that the banks adopted inconsistent and generally narrow approaches to liability, reimbursement and compensation.

Amount of scam reimbursement and compensation

During the period 1 July 2021 to 30 June 2022, the banks paid a combined total in reimbursement and/or compensation of approximately $21 million. The effect of this was that customers were impacted by the overwhelming majority (around 96%) of scam losses.

The reimbursement and/or compensation rate varied but was low across the individual banks, ranging from two to 5%.

Across the three banks for which data was available, between 1 July 2021 and 30 June 2022, there was reimbursement and/or compensation paid for around 11% of the cases when there was a scam loss (because the proceeds could not be fully recovered). When there was reimbursement and/or compensation paid to a scam victim, on average of 36% of the customer's loss was refunded.

Bank-wide policy for determining scam loss liability and reimbursement or compensation

To support fair and consistent customer outcomes, banks should have in place a bank-wide policy or approach to determining scam loss liability, and reimbursement or compensation.

We found that none of the banks had a bank-wide policy for determining scam loss liability and reimbursement or compensation. The liability-related policies we saw were generally limited in scope (e.g. to a particular type of scam typology) and/or limited to a particular business unit.

For most banks there were different policies about scam liability and reimbursement for the scams team, compared to the complaints team. Only one bank advised that the same approach is taken to determine liability, reimbursement, or compensation by both the scams team and complaints team, but it did not have this approach fully documented. Another bank advised that they have work underway to implement a consistent bank-wide approach to liability and reimbursement or compensation, and to ensure their staff consider all factors relating to the scam case and transaction when applying that approach.

Bank approaches to liability, reimbursing and compensating customers

To ensure fair outcomes and that they meet their obligations to customers, banks should have policies relating to liability, reimbursement and compensation for scam losses that cover the range of grounds on which a bank may be liable for scam losses.

The starting point used by the banks to determine liability and whether a customer is to be reimbursed or compensated is the ePayments Code, which outlines liability in relation to unauthorised transactions. However, the majority of scam transactions are authorised by the customer and therefore not currently covered under the liability principles in that code.

The ePayments Code is not the only basis on which a bank may be liable for a scams transaction such that it will need to reimburse a customer.

During the review we found other potential sources of liability that banks had considered, including:

- contractual obligations
- the implied contractual warranty in s12ED of the ASIC Act that financial services will be provided with due care and skill
- AFCA's approach to similar matters (noting that under AFCA's rules, when determining a complaint, an AFCA decision maker must do what they consider is fair in all the circumstances, having regard to legal principles, applicable industry codes or guidance, good industry practice and previous relevant determinations), and
- the obligation in s912A of the Corporations Act to do all things necessary to ensure that financial services are provided efficiently, honestly and fairly.

The potential liability of the bank in any given scam case will depend on the individual circumstances of that case. Noting the potential sources of liability above, we observed scenarios the banks had set out where the banks considered they may be liable for and/or pay reimbursement or compensation. These scenarios were mainly observed in the banks' complaint related documents or in complaints processes considered as part of our case study review (see *Customer complaints*). The scenarios included where there is:

- failure to warn the customer that the bank does not check the account name against the account number and BSB
- failure to identify or exercise due care in dealing with a customer experiencing vulnerability
- failure or delay in making reasonable inquiries with the customer where the bank was on notice that the customer is potentially being defrauded
- errors made, or delays in, attempting to recall funds from the other financial institution which impacted on recovery outcomes
- failure to apply policies or processes that may have had an adverse impact on the customer, and
- other bank errors, such as allowing the customer to transact on an account which has an alert on it advising staff to seek assistance that was ignored.

However, the banks were not consistent in taking all these grounds into account and, in general, we found that when it is confirmed that a customer has been the victim of a scam, the banks tended to adopt a narrow approach to considering liability, and reimbursing or compensating customers. For example, the banks often only consider the ePayments Code, and in some cases the scam typology, without

going on to consider other potential sources of liability and factors that may warrant reimbursing or compensating the customer.

One example of the narrow approach taken to determining liability that we saw is outlined in the case study below. It shows an 81-year-old customer who is a repeat scam victim who had a block placed on their account, being allowed by the bank to withdraw $8,000. The bank did not appear to consider these factors when it declined any liability for the transaction and advised the customer that the transaction was 'deemed as authorised', and therefore the customer was liable. Ultimately an AFCA determination was made partly in favour of the customer.

Case study: Bank's response to 81-year-old bank scam victim

In March 2021, the bank detected three payments of concern and placed blocks on the customer's accounts, after the transactions were processed, and attempted to contact the customer. Despite blocks on the account, the 81-year-old customer attended the bank's branch and withdrew $8,000 and deposited it into another bank's account (not in the customer's name).

The scam was later confirmed with the customer through a conversation that occurred in a bank branch shortly after the withdrawal. After receiving an initial SMS acknowledgement, and then two automatic and similar SMS updates in April 2021, no further updates were provided to the customer. At this stage, no reimbursement had been offered to the customer, despite the bank allowing the customer to make a withdrawal while a block had been placed on their account.

In May 2021, the customer lodged a complaint with AFCA. During this process, the bank offered the customer $8,000 as a goodwill commercial offer. This offer was not accepted by the customer and the matter resulted in AFCA making a determination which required the bank to pay the customer $8,000 for the financial loss and $500 compensation. The bank was held not liable for the initial three transactions that were processed.

Customer complaints about scams

Outcomes for scammed customers should not be dependent on whether or not they choose to raise a complaint in relation to their case. It is important that banks consider whether it is appropriate to compensate customers who fall victim to a scam regardless of whether a complaint is lodged.

Across the banks, between 1 July 2021 and 30 June 2022, around 15% of scam victims made a complaint to their bank about the matter. We found that although still a low percentage, customers who made a complaint were more likely to receive some form of compensation from the bank, compared to customers who did not.

One contributing factor to low reimbursements appears to be that staff in the scams response teams for some banks have less scope or authority than those in complaints teams. Supporting this, we found that there was greater guidance in the policies and procedures for handling scams complaints about when a complaints handler may provide reimbursement or compensation, including merit-based and commercial, or for goodwill reasons, than there was in the policies and procedures supporting scams team members in the initial resolution of scam matters.

For one of the case studies, we listened to a call where a scams team member actively encouraged and coached a customer to make a complaint if the bank could not recover their funds from the other financial institution. This suggested some level of disempowerment of staff members in that team to consider alternative grounds on which it may be appropriate to reimburse or compensate a customer. This example also appeared to be inconsistent with Regulatory Guide 271 *Internal dispute resolution* (RG 271), which outlines that a customer should not be required to express their dissatisfaction in a particular way for a bank to treat a matter as a complaint.

We note there are other factors that likely also contribute to better outcomes for customers who make a complaint, including banks making commercial decisions to pay compensation (sometimes on a 'goodwill' basis).

Overall, we observed that 37% of scammed customers who lodged an internal complaint received some form of reimbursement and/or compensation. While, across three of the banks whom data was available, 68% of customers who escalated their complaints to AFCA received some form of reimbursement and/or compensation.

Comparative snapshot of key findings

Table 1 summarises the banks' progress in relation to the key areas that we examined as part of our review.

Table 1: Comparative snaphot of key findings, by number of banks

Observation	Implemented	Partially Implemented	Not Yet Implemented	Notes
Scams strategy, governance and reporting				
› Bank had a bank-wide scams strategy	1	1	2	'Partially implemented' included one bank that although not having a documented scams strategy, had a scams uplift forum and program which collectively included most of the key elements of a strategy.
› Bank had board and senior management oversight of scams prevention, detection and response activities	4	0	0	Not applicable
› Bank had regular reporting to board and senior management	3	1	0	Not applicable
› Bank's reporting to board and senior management included a focus on customer experience and outcomes	2	0	2	Not applicable
› Bank systems captured and could automatically report on end-to-end scams cases	0	4	0	All of the banks had scams systems but these are supplemented with manual processes to obtain an end-to-end view.
› Bank had conducted an end-to-end scams review in the past three years	1	1	2	'Partially implemented' included one bank that although not having an end-to-end scams review, had undertaken a review of scam related customer conversations.

Observation	Implemented	Partially Implemented	Not Yet Implemented	Notes
Preventing scams				
› Bank had scam awareness education activities	4	0	0	Not applicable
› Bank monitored and measured the effectiveness of scam awareness education activities	0	1	3	'Partially implemented' included one bank that had implemented measures to test the effectiveness of some, but not all, of their scam awareness education activities.
› Bank had added scam-prevention friction in the provision of banking services across all channels and networks	0	4	0	Not applicable
› Bank had implemented controls to minimise misuse of bank's telephone numbers and bank's SMS alpha tags	0	3	1	'Partially implemented' included banks who had implemented controls to minimise the misuse of some, but not all, of the bank's telephone numbers and SMS alpha tags.
Detecting and stopping scams				
› Bank had ability to hold payments in real-time across all payment channels and networks	0	4	0	Not applicable
Responding to scams and scam victims				
› Bank had documented end-to-end processes and procedures for responding to a scam and a scam victim	0	4	0	'Partially implemented' included banks that had documented some but not all of their end-to-end processes and procedures for responding to a scam and scam victim.
› Bank's case studies practices aligned with bank's scam processes and procedures	0	4	0	'Partially implemented' included banks with their case studies 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 studies practices aligned with these processes and procedures.	0	4	0	'Partially implemented' included banks who had processes and procedures OR case studies practices aligned with these processes and procedures, but not both.

Observation	Implemented	Partially Implemented	Not Yet Implemented	Notes
Liability, reimbursement and compensation				
› Bank had a bank-wide policy for determining scam loss liability and reimbursement or compensation	0	1	3	'Partially implemented' included one bank who although not having a fully documented bank-wide scam liability policy, had one bank-wide approach.
› Bank's policies in relation to scams loss liability outlines all the grounds on which a bank might be liable	0	4	0	'Partially implemented' included banks that had outlined some, but not all, of the grounds on which they may be liable for scam loss.

Key terms and related information

Key terms

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
ASIC Act	*Australian Securities and Investments Commission Act 2001 (Cth)*
Banking Code of Practice	The Banking Code of Practice, dated 1 March 2020 (revised 5 October 2021)
Corporations Act	*Corporations Act 2001 (Cth)*, including regulations made for the purposes of that Act
ePayments Code	A voluntary code of practice that regulates electronic payments
IDR	Internal Dispute Resolution
PayID	Refers to a service in which bank accounts are linked to a mobile number or email address, enabling payers to confirm the payee is the intended recipient of the funds
phishing	A situation in which a scammer sends fraudulent emails or text messages that appear to look like a legitimate business in order to solicit personal information
reimbursement and/or compensation	For the purpose of this report, a payment made to the scammed customer by the bank, excluding scam loss recovered
reimbursement/ compensation rate	The percentage of scam loss after any amounts recovered that is paid to the scammed customers by the bank
RG 271	ASIC Regulatory Guide 271 *Internal dispute resolution*
s12ED (for example)	A section of the ASIC Act, in this example numbered 12ED
s912A (for example)	A section of the Corporations Act, in this example numbered 912A
scam	Type of fraud, usually with the purpose of getting money or information from people using a deceptive scheme or trick

scam loss	The net loss after any recoveries of scam proceeds and any reimbursement and/or compensation
scam loss recovered	Scam funds returned from the recipient's account to the scammed customer after the scam transaction has occurred
SMS	Short message service

Key data

Table 2: Key scams data for four major banks1 July 2021 to 30 June 2022

Scam calculation	Transaction value
Scam transactions	$845m
Less scam transactions detected and stopped	($109m)
Less scam loss recovered	($111m)
Scam loss excluding reimbursement and/or compensation	$579m
Less reimbursement and/or compensation	($21m)
Scam loss for which customer was liable	$558m

Note 1: Values are based on our analysis of data provided by the major banks.

Note 2: Scam transactions may also include payments declined due to other non-scam related factors such as insufficient funds or exceeding daily limit. Scam loss will therefore not reconcile to the Scam transactions value.

Note 3: Scam transactions excludes scams that were attempted but prevented by the bank prior to the customer performing the transaction.

Related information

Headnotes

Scams, complaints, banks

Legislation

Australian Securities and Investments Commission Act 2001

Corporations Act 2001

ASIC documents

RG 271 *Internal dispute resolution*

ePayments Code