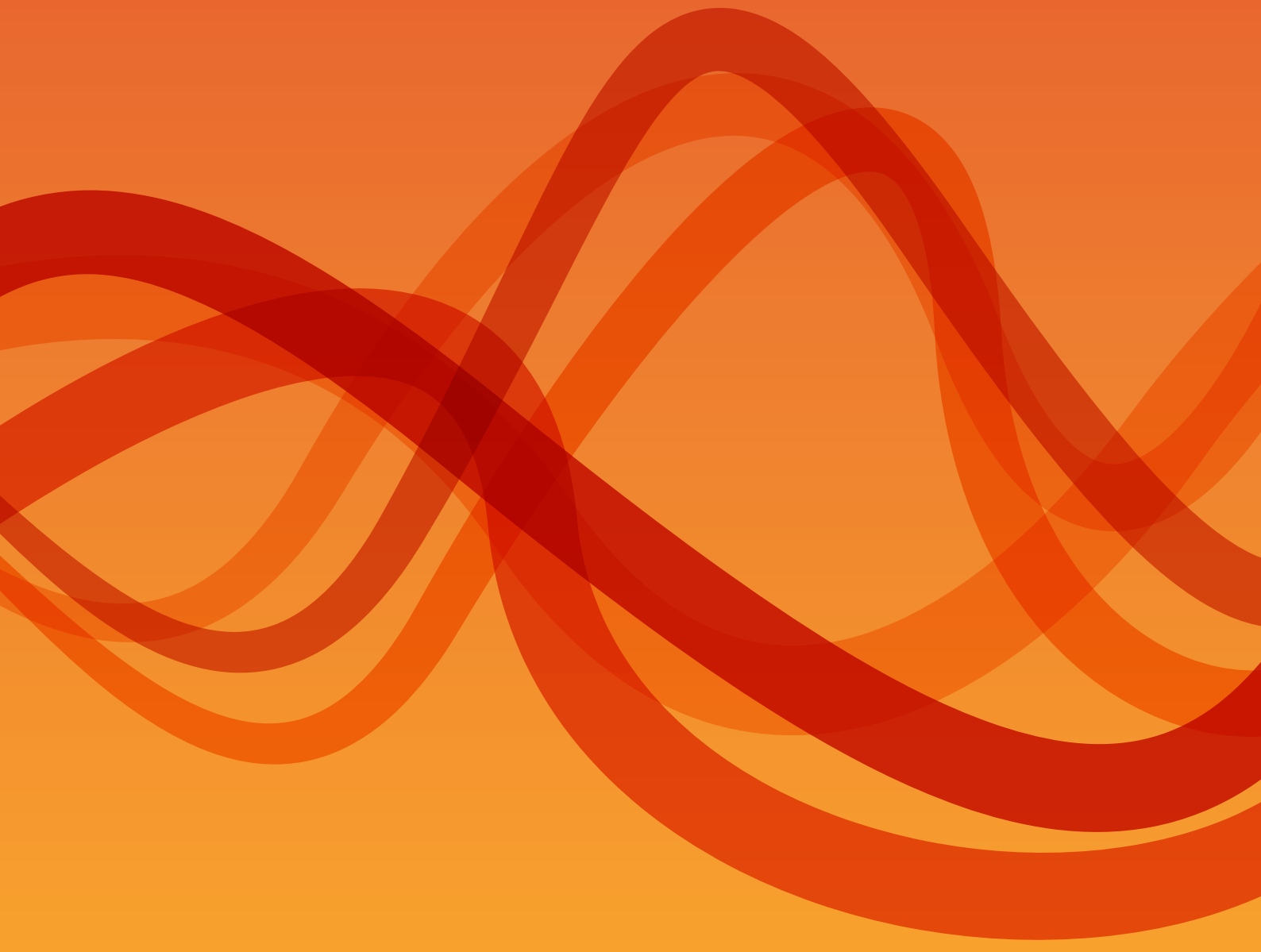
BCCC
Banking Code
Compliance Committee

Compliance with the **Banking Code of Practice**

July to December 2022



Contents

Chair's message

While fewer breaches of the Code in certain areas was pleasing, increases related to responsible lending, complaints handling and branch closures were of concern in this reporting period.

These obligations offer important protections for customers and, when breached, can have serious consequences.

This result shows again the need for banks to undertake further work. Improvements to systems and processes should be a focus as banks commit to fewer breaches and better outcomes for customers.

Pleasingly, we saw a reduction in breaches of obligations for joint accounts, direct debits and guaranteeing a loan.

In our last report, we highlighted risks with not acting on requests from vulnerable customers to change the authority on joint accounts. Control over accounts is critical for these customers and the obligations to act on such requests are fundamental to consumer protection. We welcome the improvement in compliance since the last report.

Improve compliance reporting

The data from Compliance Statements is a valuable source of information for banks and the public, so we are working hard to improve the data collection process and the way we report on the data.

In consultation with the ABA, we continue to make progress on introducing materiality thresholds for breach reporting, aligning our data classification categories with ASIC's breach reporting, and finalising criteria for benchmarking.

These developments will improve the Compliance Statement processes for banks and improve the reports that we publish, producing better insights into risk areas for banks and consumers.

We look forward to finalising these initiatives in consultation with the ABA and the industry.

Ian Govey AM
Independent Chairperson
Banking Code Compliance Committee

Introduction

The biannual Compliance Statement is an essential part of how we monitor compliance with the Code.

In the Compliance Statement, banks must provide data about their breaches of the Code, reporting on the preceding six-month period.

This report summarises the data from the six-month period of July–December 2022.

Banks must report the total number of breaches they identified during the reporting period, as well as the details of a sample of incidents that meet certain criteria.

For the sample incidents, we require details of each breach. Banks must describe the incident, event or action and then list one or more Code obligations that were breached.

The data in this report has been de-identified.

Snapshot

July to December 2022

Breaches
↑3%

This follows the **38% decrease** in the last reporting period.

Chart 1: Trend in total breaches

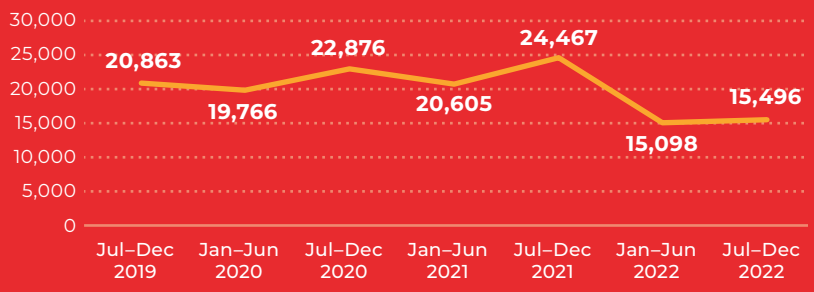
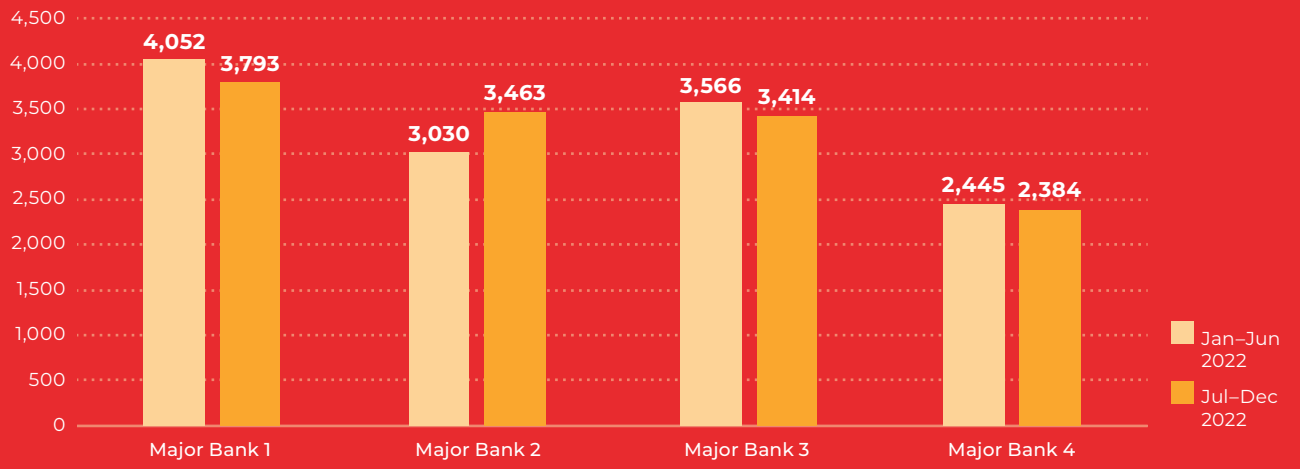


Chart 2: Breaches by the 4 major banks



The four major banks accounted for **84% (13,054) of the breaches** reported in this period.

Three of the four major banks reported a **decrease in breaches**.

Twelve of the 13 other banks reported an **increase in breaches**.

Nine million affected customers (up from 5.2 million in the last period).

$56.2 million financial impact

Down from $72.5 million in the last period.

Based on a sample of 6,193 breaches (compared to a sample of 7,483 breaches used in the last period).

Table 1: Most breaches by Code Part

Code Part		Jul–Dec 2022		Jan–Jun 2022	
		Breaches	Change	Breaches	Change
Pt 02	Your banking relationship	6,423	↑ 5%	6,131	↓ 14%
Pt 03	Opening an account and using our banking services	2,366	↓ 2%	2,414	↓ 30%
Pt 05	When you apply for a loan	2,065	↑ 12%	1,843	↓ 54%
Pt 09	When things go wrong	1,857	↓ 7%	1,989	↓ 57%
Pt 10	Resolving your complaint	1,751	↑ 19%	1,466	↓ 33%
Pt 08	Managing your account	495	↓ 19%	611	↓ 55%
Pt 04	Inclusive and accessible banking	468	↓ 14%	546	↓ 56%
Pt 07	Guaranteeing a loan	55	↓ 35%	84	↓ 32%
Pt 06	Lending to small business	16	↑ 14%	14	↓ 96%
Pt 01	How the Code works	0	0%	0	↓ 100%
Total		**15,496**	**↑ 3%**	**15,098**	**↓ 38%**

Table 2: Top 5 Code Chapters with the most breaches

Code Chapter		Breaches	Change from previous period
Ch 05	Protecting confidentiality	3,984	↑ 14%
Ch 04	Trained and competent staff	2,432	↓ 8%
Ch 17	A responsible lending approach	2,060	↑ 14%
Ch 09	Communication between us and you	1,222	↑ 8%
Ch 48	How we handle your complaint	1,170	↑ 19%

Table 3: Notable increases in breaches by Code Chapter

Code Chapter		Breaches	Change from previous period
Ch 31	Statements we will send you	60	↑ 233%
Ch 47	If you have a complaint about us	581	↑ 21%
Ch 48	How we handle your complaint	1,170	↑ 19%
Ch 14	Taking extra care with customers who may be vulnerable	384	↑ 18%
Ch 17	A responsible approach to lending	2,060	↑ 14%

Table 4: Notable decreases in breaches by Code Chapter

Code Chapter		Breaches	Change from previous period
Ch 15	Banking services for people with a low income	32	↓ 77%
Ch 34	Direct Debits and recurring payments	133	↓ 41%
Ch 41	We will try to help you if you are experiencing financial difficulty	283	↓ 16%
Ch 08	Providing you with information	656	↓ 14%
Ch 04	Trained and competent staff	2,432	↓ 8%

General findings

Breach sample

For each reporting period, we ask banks to provide additional details of a sample of breaches. These details include information about the nature, cause, impact of the breaches, and how they were corrected.

Where this report refers to 'financial impact', this means either actual or estimated financial impact on the customer or the bank at the time of reporting.

For July–December 2022, from the total **15,496 breaches**, banks provided details for a sample of **6,193 breaches** that came from **3,652 incidents**.

Cause of breaches

Human error being reported as the most common cause of breaches indicates potential issues in two areas:

- staff capability and training
- breach analysis and reporting.

Banks attributed 4,929 breaches (80%) to human error in the breach sample for July–December 2022.

Having staff sufficiently trained and capable is fundamental to complying with the Code and delivering good services and outcomes for customers.

Banks must support staff with quality training and guidance to minimise errors and prevent recurrence of breaches.

Crucial to this, though, is properly analysing the breaches and identifying their root causes.

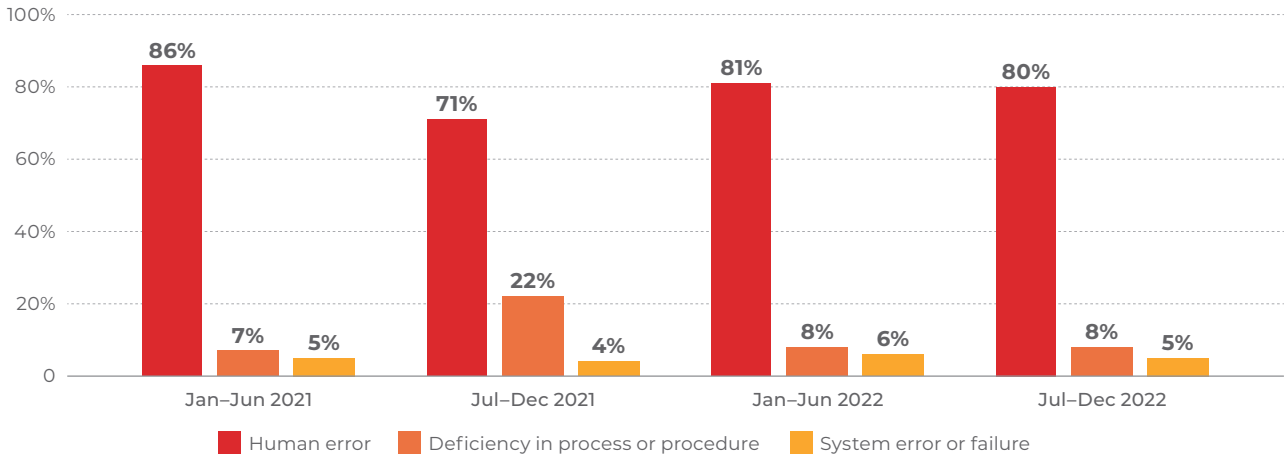
Of the 4,929 breaches where human error was reported as the cause, only 152 breaches (3%) had additional root causes identified.

We reported in Building Organisational Capability that attributing a breach to human error is a shortcut solution for a bank. In many cases, the root cause of the breach can be deeper, connected to other factors such as systems, processes, technology, training, and organisational culture.

Implementing the right solutions to reduce breaches, improve compliance with the Code, and bring about better outcomes for customers begins with quality analysis of root causes.

We urge banks to resist the attractive shortcut of attributing breaches to human error and to make the effort to find the deeper root causes.

Chart 3: Top 3 causes of breaches



Identifying breaches

Following the spike in the previous reporting period, breaches identified through customer complaints returned to a relatively typical level in July–December 2022.

We found that banks most often identified breaches through Line 1 monitoring processes (47%), with customer complaints accounting for 27%.

Changes to ASIC regulations in 2021 expanded the definition of complaint and prompted banks to adjust systems and processes in 2022. This resulted in banks finding more breaches from customer complaints.

But in refining the processes to comply with new regulations, Line 1 monitoring once again became the main way that banks identified breaches.

Identifying most breaches through Line 1 monitoring indicates that banks had a more proactive compliance approach in July–December 2022. This increases the likelihood of capturing all breaches and using them to learn and improve.

While identifying breaches from multiple sources is important, being proactive on matters of Code compliance provides critical early insights into emerging trends and risks. This can prompt a bank to act before issues arise and affect customers.

The four major banks led the return of Line 1 monitoring as the most common way to identify breaches. The other banks still identified more through customer complaints, indicating more work is needed to enhance their proactive efforts to identify breaches.

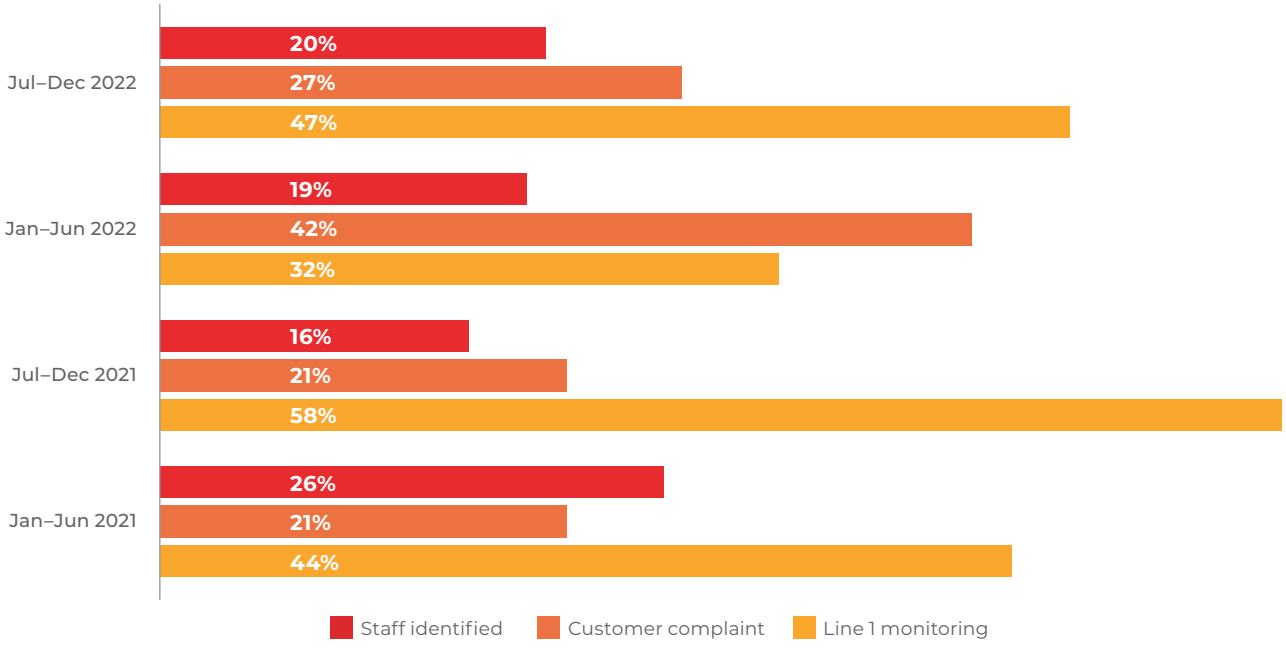
Top three methods for identifying breaches in the major banks:

- Line 1 monitoring (52%)
- Customer complaints (24%)
- Self-identified or reported by staff (18%)

Top three methods for identifying breaches in the other banks:

- Customer complaints (38%)
- Self-identified or reported by staff (29%)
- Line 1 monitoring (24%)

Chart 4: Top 3 sources for identifying breaches



Impact of breaches

Assessing the impact of breaches provides a tangible connection to customers and the real-world effects of a bank's actions. It is a reminder that every breach affects the lives of customers.

Breaches in the second half of 2022 affected nine million customers – a significant increase of 73% on the previous period (5.2 million customers).

This is a result that reflects poorly on the industry and should prompt action within banks to identify issues and implement improvements.

Although we saw an increase in the number of affected customers in July–December 2022, the financial impact decreased to $56.2 million from $72.5 million in the previous period.

The discrepancy between the affected numbers of customers and the financial impact can vary depending on the specifics of the breaches in any given period.

To illustrate this, one bank reported a breach affecting 1.5 million customers without a financial impact.

In the context of the impact of breaches, we see that improving compliance with the Code for its own sake is not the goal. The ultimate goal of compliance is to ensure good outcomes for banks' customers.

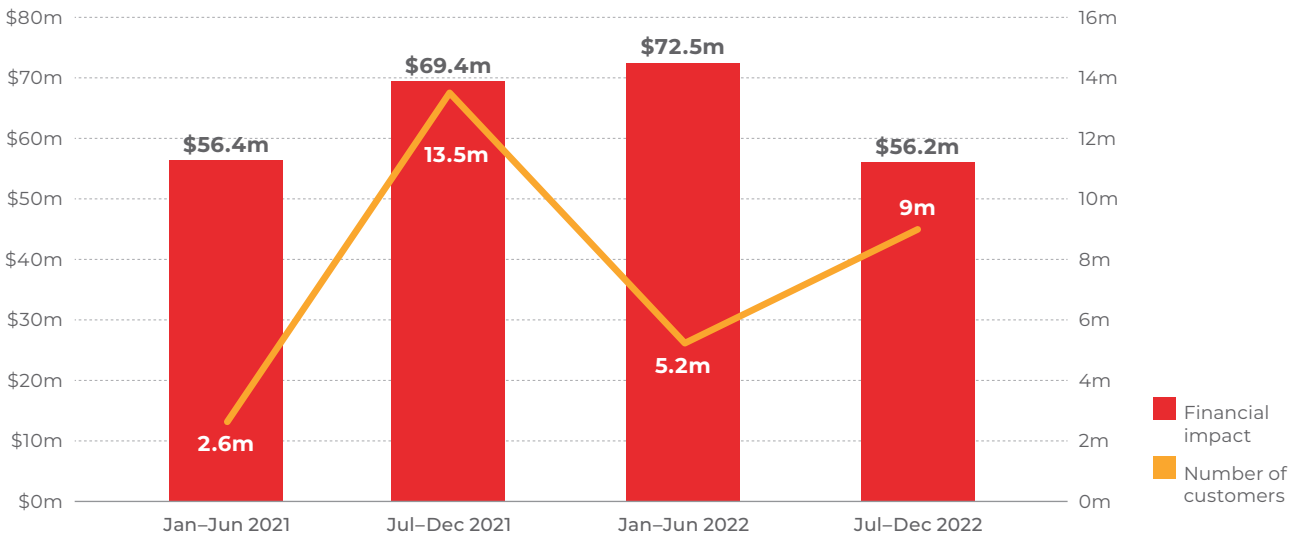
» Top three breaches by number of affected customers:

- One bank sent some customers an expired offer and others a communication thanking them for a charitable donation that they may have not made. The breach affected **1.8 million** customers and was attributed to a system error.
- One bank inadvertently allowed an adviser to access account names, numbers and balances of some customers' accounts. The breach affected **1.5 million** customers and was attributed to an internal system error.
- One bank issued demand notices with daily accrual amounts that could have been inaccurate if the interest rate changed before the payment was due. The breach affected **1.2 million** customers and was attributed to a deficiency in proces

» Top three breaches by financial impact:

- One bank approved business loans that were from fraudulent loan applications. This had a financial impact of **$14.7 million** and affected 49 customers.
- One bank incorrectly authorised multiple transactions and overdrew accounts due to defects from a system change. This had a financial impact of **$7.9 million** and affected 1,512 customers.
- One bank provided customers with agreed pricing that differed to the fees and costs disclosed in its PDS. This had a financial impact of **$2.9 million** and affected 1,665 customers.

Chart 5: Impact of breaches



Corrective action

The data indicates that banks considered breaches to be mainly isolated lapses in staff performance rather the results of deeper issues with systems and processes.

Staff training, coaching and feedback was, again, the most common corrective action in July–December 2022.

Corrective action provides an insight into how banks assess the nature of breaches. The action a bank takes in response to a breach should be linked to what it considers to be the root cause. The corrective action addresses the cause, pursues long-term solutions that prevent recurrence, and works to deliver good outcomes for customers.

While staff training, coaching and feedback is fundamental for breaches caused by human error, improvements in processes, systems and controls can get at deeper issues and reduce the risk of human error.

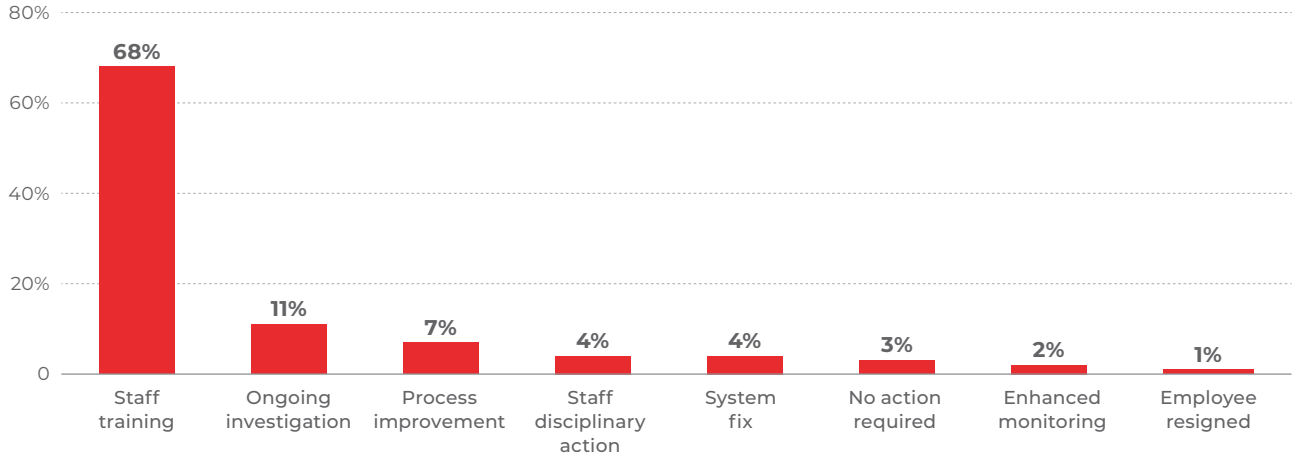
» Most common corrective action for the major banks:

- Staff training, coaching and feedback – 68%
- Process review – 6%
- System fixes – 4%

Most common corrective action for the other banks:

- Staff training, coaching and feedback – 69%
- Process review – 12%
- System fixes – 4%

Chart 6: Corrective actions taken in response to breaches (July–December 2022)



Remediating breaches

Remediation is a vital element in addressing breaches and plays a major part in a bank's relationship with a customer.

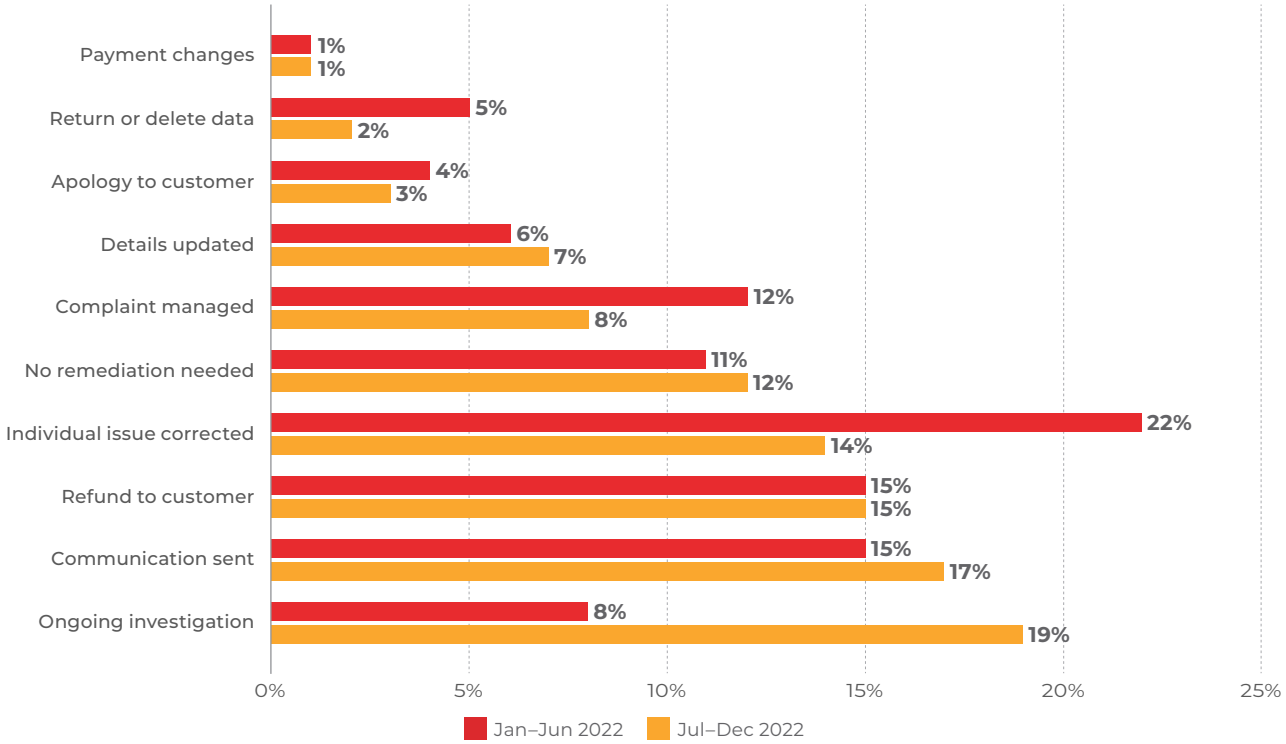
The root causes of a breach and its impact helps determine how a bank remediates a customer, but we expect that all remediation is timely, appropriate and aimed at customer satisfaction in line with Code obligations.

In July–December 2022, communicating with the customer was the most common form of remediation across the industry.

At the time of reporting, remediation was still being investigated for 19% of breaches.

This result was influenced in large part by one major bank that reported its remediation for 45% of breaches was still being investigated.

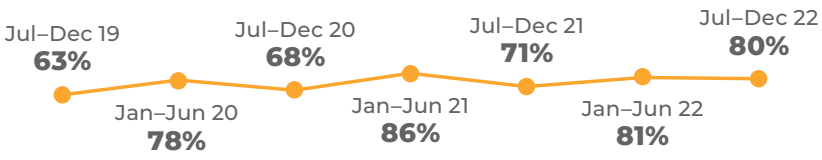
Chart 7: Remediating breaches



Spotlight on human error*

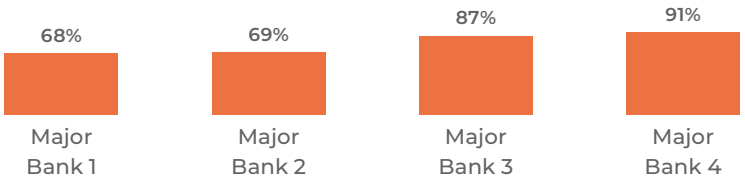
80%

of breaches caused by human error



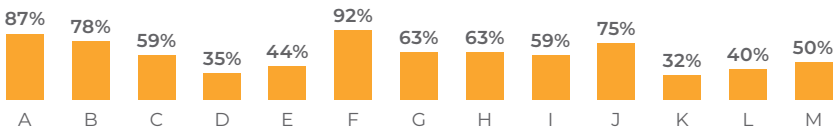
*Based on a sample of 6,193 breaches (compared to a sample of 7,483 breaches used in the last period).

Breaches caused by human error in July–December 2022



4 major banks

Other banks
(A–M)



We urge banks to analyse breaches thoroughly to identify the root causes and make improvements to rectify them and prevent recurrence. Attributing breaches to human error as the easy default option is poor practice.

In cases where human error has played a part, it is common that staff were influenced or constrained by systems and processes, technology, training or organisational culture.

Top breaches attributed to human error	Applying incorrect interest rates	Failing to record disclosure consent	Failing to protect a customer's confidentiality

Banks must continually assess infrastructure, remuneration and incentive programs to ensure they help staff achieve compliance with Code obligations and the right outcomes for customers.

Compliance with obligations

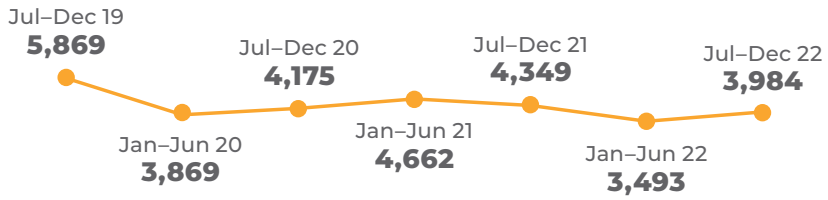
Privacy

Part 2, Chapter 5: Protecting confidentiality

Up by

14%

(↑491 breaches)



The Code provides important protections for consumer confidentiality and complements the legal obligations on privacy and information handling.

Despite the environment of heightened risk, we saw an increase in breaches of the obligation to protect confidentiality. This is concerning.

Breaches of privacy obligations was again the most common type of breach in July–December 2022.

Eleven of the 17 banks (including three major banks) reported an increase while five, including one major bank, reported a decrease in breaches of privacy obligations. One bank reported no change.

» Two major banks reported an increase in breaches of privacy obligations of 31%.

Failing to meet these obligations in the Code can lead to serious consequences for customers, especially customers experiencing vulnerability.

In turn, this can also have ramifications for a bank in remediation costs, damage to reputation and potentially legal issues.

Addressing breaches of privacy obligations is critical to ensuring good outcomes for customers, especially as risks increase.

It is imperative that banks analyse the breaches to identify the root causes and implement corrective action that provides strong sustainable solutions.

In the breach sample, banks provided further information on 794 incidents, including 906 breaches.

Of the 794 incidents, 698 contained breaches solely of Chapter 5 (798 breaches). The remaining 96 incidents contained breaches of Chapter 5 and other chapters of the Code (108 breaches).

These incidents affected 2.1 million customers and had a financial impact of $3.3 million.

Banks attributed 80% of the privacy breaches to human error. They identified most of the breaches through Line 1 monitoring and customer complaints.

Staff training, coaching and feedback was the corrective action for 80% of these breaches.

Remediation varied:

- No customer remediation – 17%
- Communicating with customers – 15%
- Personal information either destroyed, deleted or returned – 14%

Table 6: Breaches of Chapter 5 that affected large numbers of customers

Customers affected	Incident
1.5 million	One bank's adviser had unauthorised access to account names, numbers and balances of accounts due to a system error.
242,000	In one bank, customer information was accessed, used or disclosed without authority due to a system error.
60,000	One bank sent emails with attachments to the wrong recipients due to human error.
48,000	One bank disclosed the tax file numbers of customers due to a deficient process.
48,000	One bank disclosed personally identifiable information of customers without authority due to human error.
30,000	A decommissioned database of one bank was subject to a data breach which was identified by a regulator and, although there was no personal information involved, reported to the OAIC.
27,000	A third-party supplier for one bank inadvertently sent files that included personal information of customers to an unrelated client due to human error.

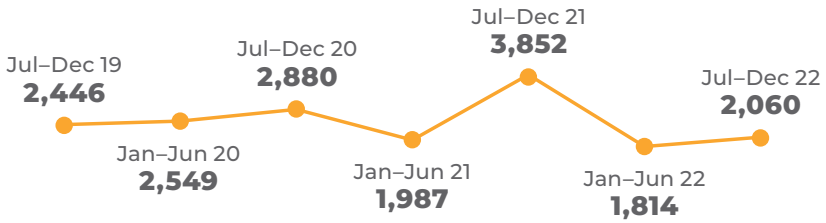
Responsible lending

Part 5, Chapter 17: A responsible approach to lending

Up by

14%

(↑246 breaches)



Economic pressures have increased the risk of customers falling into financial hardship or distress, highlighting the importance of responsible lending practices.

The Code has important obligations that complement the law to ensure banks do not provide unsuitable loans to customers. Central to this is the obligation for banks to exercise the care and skill of a diligent and prudent banker.

In the context of the current economic pressures, and following the results of the previous reporting period, the increase in breaches of the responsible lending obligations in July–December 2022 is disappointing.

It shines a light on practices that demand attention and improvements.

» Two major banks reported increases in breaches of responsible lending obligations of 59% and 31%, respectively.

The other two major banks reported decreases in these breaches of 30% and 8%.

Breaching responsible lending obligations has the potential to exacerbate financial hardship, which could be particularly severe for customers experiencing vulnerability.

Minimising breaches and strengthening compliance with these obligations in the Code will improve the outcomes for customers and mitigate potential harms that come with financial difficulty.

Banks must take the opportunity to improve. They should analyse the breaches of the responsible lending obligations and use the valuable information to identify root causes, recognise risks and implement targeted solutions.

One major bank accounted for more than half of the breaches of the responsible lending obligations. It attributed the increase to improvements in its categorising of Code breaches following the introduction of ASIC's breach reporting regime.

Another major bank attributed its increase to an improved, targeted approach to mortgage compliance reviews in 2022. Its renewed focus on staff awareness and reporting also played a role.

In explaining its reported decrease in breaches, one major bank cited its continued use of a centralised system to streamline home loan processes.

In the breach sample, banks provided further information on 419 incidents, including 1,288 breaches.

Of the 419 incidents, 366 incidents contained breaches solely of Chapter 17 (1,232 breaches). The remaining 53 incidents contained 56 breaches of Chapter 17 and other chapters of the Code.

These incidents affected 51,000 customers and had a financial impact of $6 million.

Banks attributed 91% of the breaches to human error. Human error had been the cause of at least 85% of breaches of responsible lending obligations in the last three reporting periods.

This indicates a need to renew focus on staff training and guidance to improve performance and to consider systems or process improvements to mitigate the risk of human error.

Most of the breaches were identified through Line 1 monitoring (85%).

Staff training, coaching and feedback was the corrective action for 59% of these breaches. At the time of reporting, 31% of the breaches were reported as ongoing investigation.

Correcting an individual customer's issue was the most common form of remediation, accounting for 23% of the breaches.

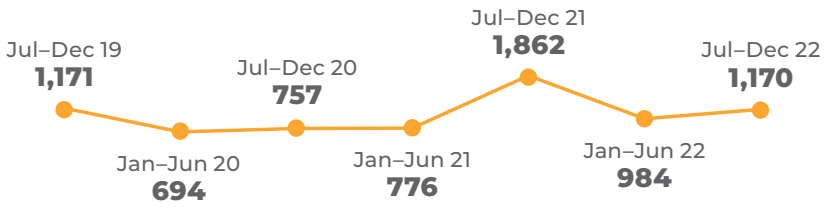
Complaints handling

Part 10, Chapter 48: How we handle your complaint

Up by

19%

(↑185 breaches)



The increase in breaches in July–December 2022 indicates that banks must do more to handle complaints fairly and promptly.

The Code requires banks to be fair and reasonable, keep customers informed and respond within certain timeframes.

Customers expect to have complaints addressed promptly and fairly, and failing to comply with the Code obligations can erode their trust and faith in banks and potentially cultivate a damaging cynicism.

Handling complaints promptly not only protects the interests of individual customers, but it also contributes to the reputation of the bank and the industry, fostering better relationships and a sector that emphasises customer needs and outcomes.

When complaints are handled properly with good records, they offer banks valuable insights into issues and trends, acting as a catalyst for change and improvements.

» Eleven banks reported an increase in breach obligations for handling a complaint, while three banks reported a decrease. Three banks reported no changes in their breaches.

Banks attributed increases to:

- greater volume of complaints
- issues with staffing and capacity
- better breach identification because of internal dispute resolution obligations.

In the breach sample, banks provided further information on 202 incidents, including 301 breaches.

Of the 202 incidents, 139 contained breaches solely of Chapter 48 (224 breaches). The remaining 63 incidents contained 203 breaches of Chapter 48 and other chapters of the Code.

These incidents affected 14,000 customers and had a financial impact of $69,000.

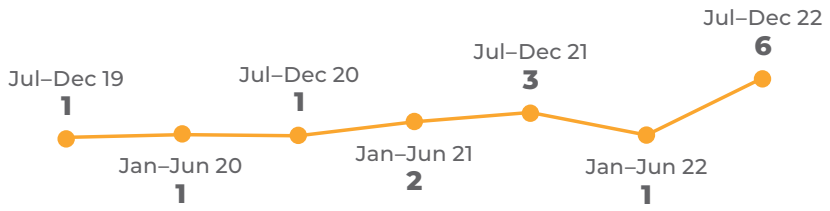
Banks attributed 71% of the breaches to human error. Staff training, coaching or feedback was the corrective action for 72% of breaches, and customer communication was the most common remediation (35%). Most breaches were identified through Line 1 monitoring (54%).

This suggests that staff training, guidance and oversight could be used more effectively to prevent the errors that lead to breaches of this kind. When supported with good systems and processes, training and guidance will work to improve performances, reduce breaches, and safeguard relationships with customers.

Branch closures

Part 2, Chapter 7: Closing a branch

6
breaches



In July–December 2022, we saw the highest number of breaches of obligations when closing a branch since the 2019 Code came into effect.

The Code mandates that banks comply with the ABA Branch Closure Protocol when closing a branch in certain circumstances. The Protocol outlines the commitment to provide banking services in remote, rural and regional areas, and the processes banks will go through, including to provide written notices, when closing a branch where there is no access to alternative banking services.

Complying with these obligations is crucial to safeguarding the needs and interests of customers in remote, rural and regional areas.

Breaching the obligations disrupts access to essential financial services for thousands of people in communities that are often disadvantaged. This erodes trust, damages a bank's reputation, and hinders financial inclusion.

Adhering to the Code obligations demonstrates a commitment to strengthen customer relationships, foster a more inclusive banking environment, and deliver positive outcomes.

We know that banks are closing branches in increasing numbers and we expect that they have the systems and processes in place to comply fully with their obligations to minimise the impact on communities.

Two major banks accounted for all the breaches, which affected over 5,000 customers.

The breaches included:

- failing to provide the required written notice of intention to close a branch
- failing to waive any fees and charges associated with accessing alternative banking services.

It is paramount that these banks properly analyse their breaches and make the necessary improvements to ensure they do not repeat them.

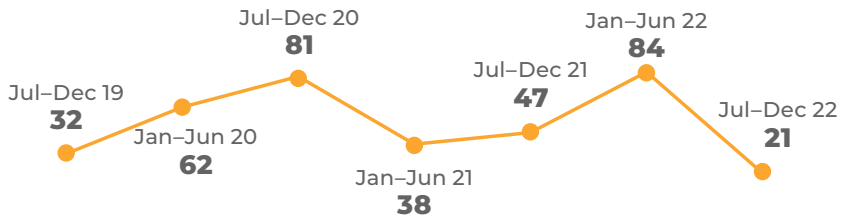
Joint accounts

Part 8, Chapter 35: Joint accounts

Down by

75%

(↓63 breaches)



The decrease in breaches of obligations for joint accounts was a welcome result from the July–December 2022 reporting period.

The Code requires banks to explain to customers how joint accounts work and, when asked, to change the account authority so that all holders must approve future withdrawals.

The latter is a critical point for customer protection, especially for people experiencing vulnerability.

Complying with these obligations helps prevent misunderstandings, disputes and, in more extreme cases, abuse for customers. They offer protections that have a tangible effect on the lives of these customers.

While we are pleased to see improved compliance in this area, we reiterate that it is vital that banks aim to improve further and minimise the risk of these breaches.

» Two major banks reported significant decreases in breaches of obligations for joint accounts (down by 47 breaches and 17 breaches each) and two banks reported small decreases (down by one breach each).

Three banks reported small increases (up by one breach each). Twelve banks reported no breaches of joint account obligations.

In the breach sample, banks provided further information on 11 incidents including 12 breaches.

Of the 11 incidents, nine contained breaches solely of Chapter 35 (10 breaches). The remaining two incidents contained three breaches of Chapter 35 and other chapters of the Code.

These incidents affected 16 customers and had a financial impact of $308,000.

All 12 breaches were of the obligation to change the account authority so that all holders must approve future withdrawals.

Example of breaches:

- One bank allowed one account holder to transfer funds out of a joint account without the approval of the other account holder. This resulted in a financial impact of $151,504.
- One bank failed to apply restrictions to a joint account after being notified of a dispute between the account holders. This resulted in a financial impact of $95,000.
- One bank processed a redraw from a joint home loan with only one borrower's signature. This resulted in a financial impact of $28,000.
- One bank changed the authority on a joint account without the approval of both account holders. This resulted in a financial impact of $50.
- One bank failed to change the signing authority on a joint account. The bank reported no financial impact from this breach.

While the financial impact from such breaches varies, the breaches place customers in vulnerable positions and can have severe consequences.

Banks need to review their processes for managing joint accounts to ensure they comply with the Code and do not contribute to customer harm.

Banks attributed 92% of the breaches to human error. Most of the breaches were identified through customer complaints (58%) and communicating with the customer was the most common form of remediation (33%).

Banks corrected more than half (58%) of the breaches with training, coaching or feedback, highlighting the need to improve training and guidance to minimise future errors.

Reviewing and improving processes was the corrective action for a quarter of these breaches (25%).

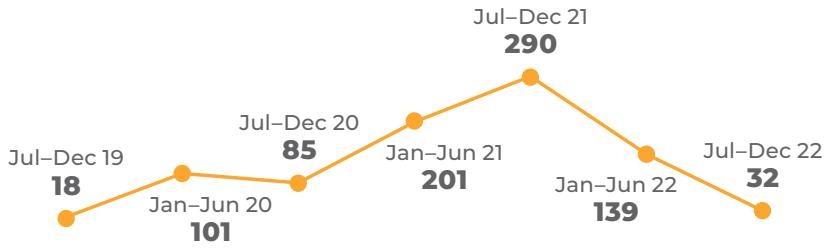
Customers on a low income

Part 4, Chapter 15: Banking services for people with a low income

Down by

77%

(↓107 breaches)



The reported reduction in breaches signifies an improved commitment by banks to support and cater to the financial needs of vulnerable customers.

The obligations in Chapter 15 of the Code aim to ensure that banks offer accessible, affordable, and appropriate banking services tailored to the specific circumstances of low-income individuals, promoting financial inclusion and fair treatment within the banking industry.

» Six banks reported a decrease in breaches of obligations for services for people with low incomes and 11 banks reported no breaches.

In the breach sample, banks provided further information on 13 incidents including 16 breaches.

Of the 13 incidents, seven contained breaches solely of Chapter 15 (eight breaches). The remaining five incidents contained eight breaches of Chapter 15 and other chapters of the Code.

These incidents affected 230 customers but had no reported financial impact.

The breaches included:

- failing to enquire about the customer's circumstances
- failing to raise the option of low- or no-fee account when relevant.

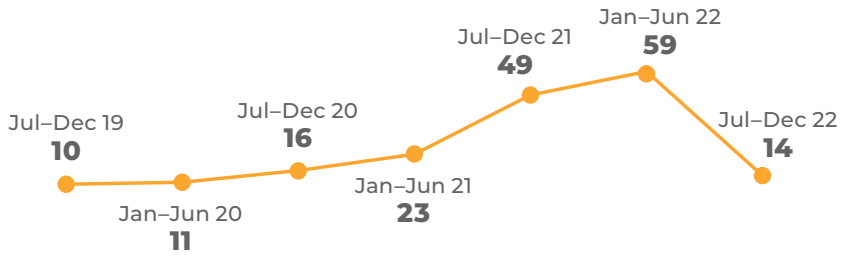
Basic accounts

Part 4, Chapter 16: Basic accounts or low- or no-fee accounts

Down by

76%

(↓45 breaches)



This is the first reporting period in which we saw a decrease in breaches of obligations for basic accounts.

The obligations require banks to raise awareness and promote basic, low- or no-fee accounts to eligible customers.

They are an important consumer protection that ensure banking services are affordable and accessible to low-income customers, reducing the risk of exacerbating financial hardship and harm.

» One bank reported a 96% decrease in breaches of obligations for basic accounts and two other banks reported small decreases.

Two banks reported an increase in breaches while 12 banks reported no changes in breaches.

In the breach sample, banks provided further information on 11 incidents including 12 breaches.

Of the 11 incidents, two contained breaches solely of Chapter 16. The remaining nine incidents contained 10 breaches of Chapter 16 and other chapters of the Code.

These incidents affected 1,760 customers and had a financial impact of $7.9 million.

This impact, however, is largely the result of breaches from an incident in one bank. The bank reported that, due to a system change, it incorrectly authorised multiple transactions and overdrew accounts. This led to breaches that affected 1,500 customers and accounted for nearly all of the $7.9 million in financial impact.

Examples of breaches:

- A staff member in one bank failed to promote low- or no-fee accounts despite knowing that the customers had concession cards. This was attributed to human error and affected eight customers.
- One bank incorrectly processed a customer's request to switch from a transaction account to a basic account, which led to the customer incurring dishonour fees.
- One bank incorrectly switched 14 customers to a fee-carrying account instead of a basic no-fee account. The bank identified the breach through customer complaints and attributed the cause to insufficient staff training.

Banks attributed 83% of the breaches to human error. They identified most of the breaches through Line 1 monitoring.

Communicating with the customer was the action to remediate customers for half of the breaches, and staff training was the corrective action for 92% of the breaches.

» The decreases in the breaches of Chapter 15 and 16 that banks self-reported do not align with the findings of ASIC's review of target market determinations for high-fee and low-fee accounts offered by some banks.

The Better Banking for Indigenous Consumers Project reviewed a sample of banks and found many indigenous customers had high-fee accounts, despite being eligible for low-fee basic accounts.

Although banks were aware of many customers being eligible for low-fee accounts, their processes to transfer the customers to the low-fee accounts were ineffective.

These findings placed a spotlight on the obligations of Chapter 15 and 16 of the Code.

While the project focused on indigenous customers, it has implications for all customers eligible for low-fee accounts.

Minimising financial hardship and harm is paramount in pursuing good outcomes for customers and we expect banks make greater and consistent efforts to raise awareness of, and offer, fee-free accounts to all eligible customers.

Given the apparent discrepancy between the findings of ASIC's review and the decrease in breaches reported, we are concerned that banks are not accurately identifying and reporting these obligations in Compliance Statements.

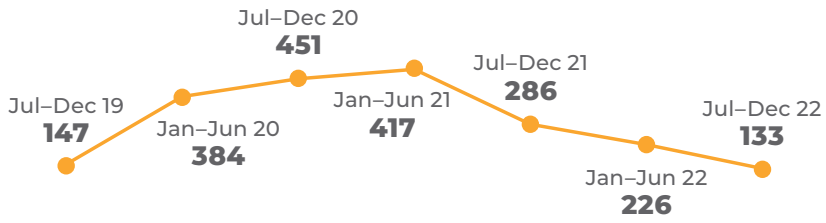
Direct debits

Part 8, Chapter 34: Direct debits and recurring payments

Down by

41%

(↓93 breaches)



The downward trend in breaches indicates that banks are gradually improving compliance with direct debit obligations. Breaches in July–December 2022 are the lowest since the Code came into effect in 2019.

The Code requires banks to promptly act on requests to cancel direct debit payments, investigate unauthorised direct debits and provide customers with their direct debits and recurring payments when requested.

The obligations for direct debits and recurring payments are important as they protect customers from unauthorised transactions, ensure transparency in payment processes, and foster trust in banking services.

Better compliance with these obligations leads to a decrease in likelihood of financial disputes and potentially financial hardship, contributing to a better banking service for customers.

However, the improvements have been slower than we expected.

Over the years, we have made great efforts to focus on monitor compliance and support banks with direct debit obligations.

- **Compliance update: cancellation of direct debits**, September 2021
- **Direct debit compliance update**, September 2019
- **Report: Improving banks' compliance with direct debit cancellation obligations**, October 2017 (published as Code Compliance Monitoring Committee)
- **Inquiry report: Direct Debits follow-up**, May 2012 (published as Code Compliance Monitoring Committee)
- **Inquiry report: Direct Debits**, June 2009 (published as Code Compliance Monitoring Committee)

Direct debit services are expected to become less common as banks provide customers with the more advanced payment service option PayTo.

PayTo is an improved payment system that provides an account holder with more control over their funds.

We are monitoring the implementation of PayTo with its anticipated benefits to customers. As it is rolled out, we expect banks to continue to comply with direct debit obligations to support customers who remain on direct debit services.

» Eight banks reported a decrease in direct debit breaches and three reported an increase.

Six banks reported no breaches of these obligations.

In the breach sample, banks provided further information on 33 incidents including 68 breaches.

Of the 33 incidents, 22 contained breaches solely of Chapter 34 (57 breaches). The remaining 11 incidents contained 11 breaches of Chapter 34 and other chapters of the Code.

These incidents affected 500 customers and had a financial impact of $15,000.

Examples of the breaches included:

- One bank failed to provide clear information to 1,882 customers about a credit interchange which resulted in a loss of $80,482.
- One bank failed to cancel direct debits of a small business customer that resulted in the account being overdrawn. This resulted in a loss of $120,000.
- One bank failed to cancel a customer's direct debit after receiving the request, which resulted in a loss of $2,551.
- One bank failed to cancel the direct debits of 17 customers, which resulted in a loss of $1,670.
- One bank failed to cancel direct debit for a customer who was experiencing vulnerability, which resulted in a loss of $1,750.

Banks attribute 97% of the breaches to human error, an increase from the 85% in the last reporting period. They identified 53% of the breaches through Line 1 monitoring and 44% through customer complaints.

Providing customers with either a refund, a reimbursement or a goodwill payment was remediation for 32% of the breaches and banks either called or wrote to customers to rectify errors in 28% of the breaches.

With human error reported as the main cause of the breaches, banks used staff training, coaching or feedback to correct 97% of the breaches.

Spotlight

Vulnerable customers and scams

Australians lost a record $3.1 billion to scams in 2022 according to the Australian Competition and Consumer Commission's (ACCC) Targeting Scams report.

The report highlighted that Australians experiencing vulnerability or hardship in particular reported record losses. This includes people with a disability, indigenous Australians and people from culturally and linguistically diverse communities.

Our data shows an 18% increase in breaches in July–December 2022 of obligations to take extra care with customers experiencing vulnerability (59 breaches).

Part 4, Chapter 14 of the Code relates to a bank's commitment to take extra care with customers experiencing vulnerability.

It is important that extra care is provided to customers identified as at risk of being scammed.

What we saw

- A 93-year-old customer of one bank informed the bank that they gave their debit card number, expiry date, CVV, name and date of birth to someone purporting to be from NBN. The bank confirmed that no transactions had been performed at the time but failed to block the account as per its process. Separately, the bank's fraud trigger system blocked a potentially fraudulent transaction of $9,500. However, the bank incorrectly unblocked the account while awaiting the customer's confirmation about the validity of the transaction. The customer suffered a loss of $140,469.56.
- A customer attended a branch to report a remote access scam and was advised to call the next day. But because of delays on the phone, the customer was unable to stop the transfers in time. The first-time payment made by the scammer was not placed on a required security hold and this led to a loss of $47,806.61.
- One bank's fraud team locked a customer's internet banking following suspicious payments. However, further BPAY payments were made and the bank assumed they were genuine, so it removed the initial lock placed by the fraud team. This resulted in more unauthorised transactions and a loss of $105,222.08.
- One bank reported three separate incidents of first-time payments not being placed on a required security hold in line with its process. This led to three customers falling victim to a remote access scam that resulted in a combined loss of $60,683.75.
- Due to long wait times, a customer of one bank was unable to connect with the fraud team to report a scam. The resulting delay in notifying the bank meant the customer was unable to stop a payment in time and lost $59,602.84.
- One bank inadvertently removed a fraud hold on a customer's account which resulted in the customer becoming a victim of fraud and a loss of $50,000.

What we expect

Banks must comply with vulnerability obligations under Part 4 of the Code, and we encourage them to act quickly if a customer's account is at risk of being scammed.

We also encourage banks to regularly review systems and processes to ensure the controls they have in place minimise the risk of scams and are functioning as intended. In the area of scam prevention, review and continuous improvement is essential.

Any warning flags or stops placed on accounts to prevent unauthorised action should be communicated to all the relevant areas of the bank to ensure consistent action.

Inclusive and accessible banking services

Providing accessible banking services is essential for allowing all people, including some of the community's most vulnerable, to take control of their finances.

In July–December 2022, we saw a 65% increase in breaches related to inclusivity and accessibility (15 breaches).

The obligation

Part 4, Chapter 13 of the Code requires a bank to commit to providing inclusive and accessible banking services.

What we saw

- One bank's audit discovered several accessibility issues in its banking app, including issues with colour contrast, text size, labels on forms and screen-reader capabilities. This suggests many customers were unable to use the app fully, restricting their access to the bank's services.
- Staff at one bank tried to help a customer dispute unauthorised transactions online without success. The staff member emailed the customer the dispute form but did not check if the customer required assistance to complete and return the form. Due to mobility issues and difficulty using a computer, it took the customer three months to lodge his dispute. The bank was unable to recover most of the disputed transactions as a result of the time it took to receive the form. The bank reimbursed the customer for the losses.

What we expect

We encourage banks to regularly review and improve their digital banking platforms to ensure they meet high standards of accessibility. This ensures all people, in particular people experiencing vulnerability, are not restricted in using essential banking services.

When dealing with concerns for which time is critical, banks should identify this and avoid delays. Banks should allow customers to lodge disputes over the phone, especially when the customer exhibits clear signs of low digital literacy.

Breach data

Breaches of Part by Chapter

Chart 8: Breaches of Part 2 by Chapter

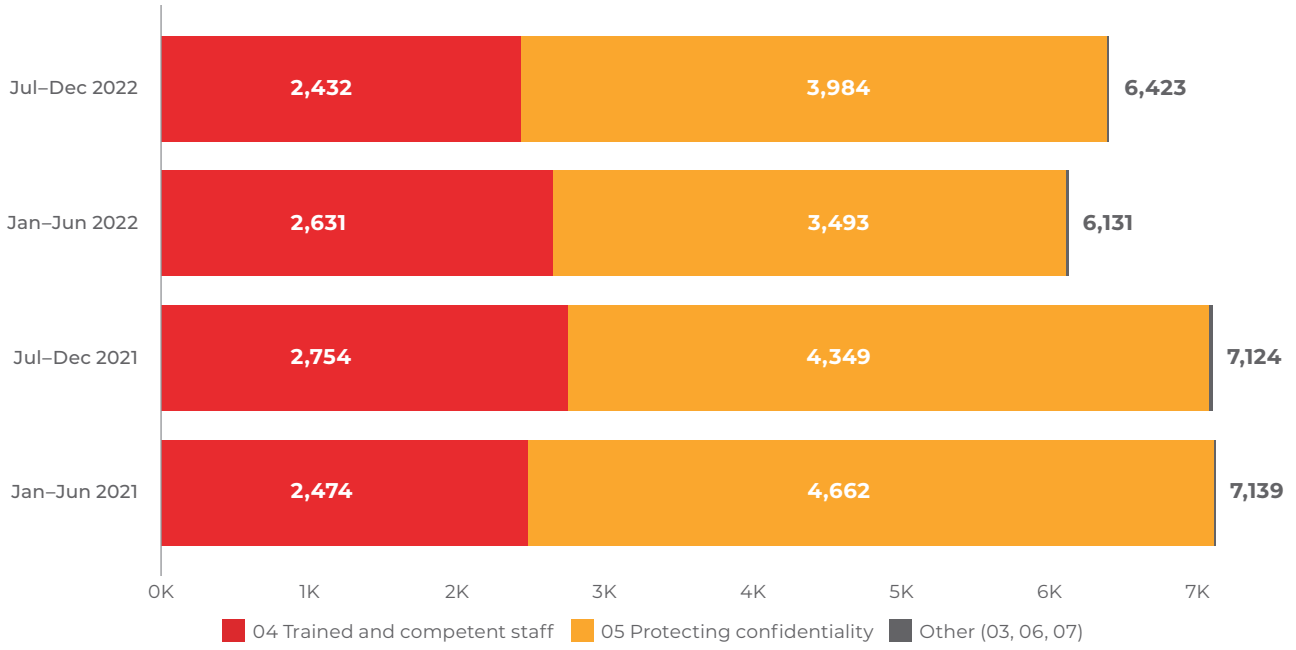


Chart 9: Breaches of Part 3 by Chapter

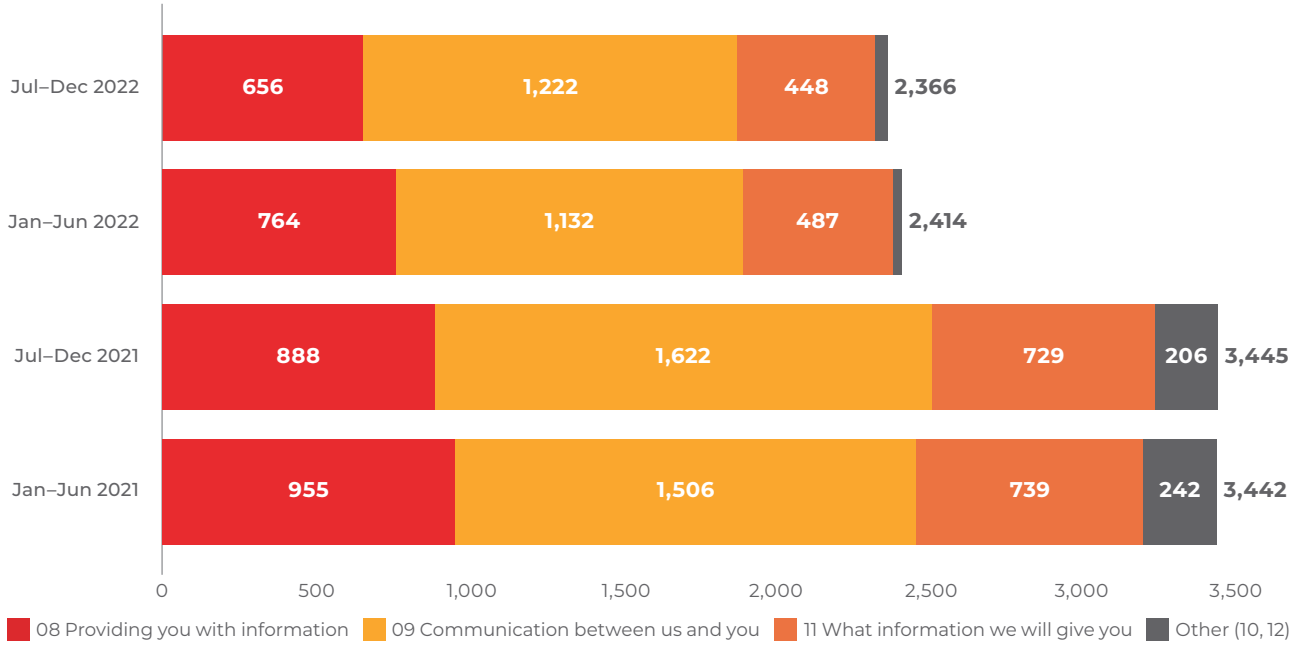


Chart 10: Breaches of Part 4 by Chapter

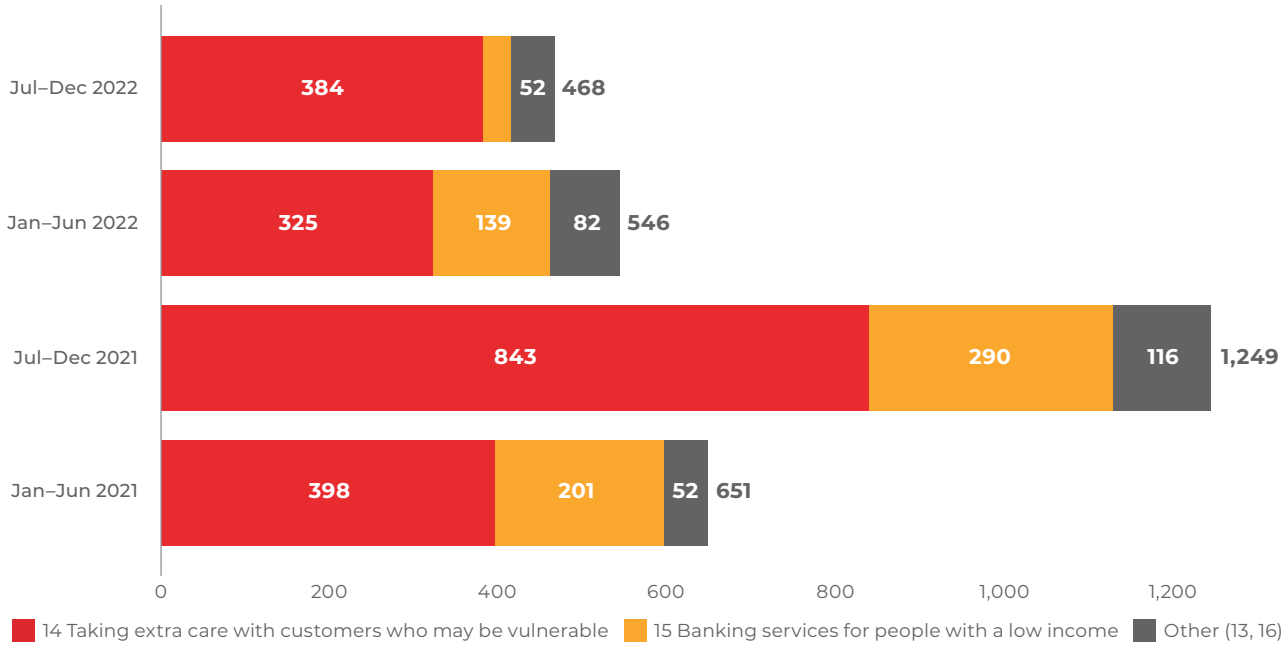


Chart 11: Breaches of Part 5 by Chapter

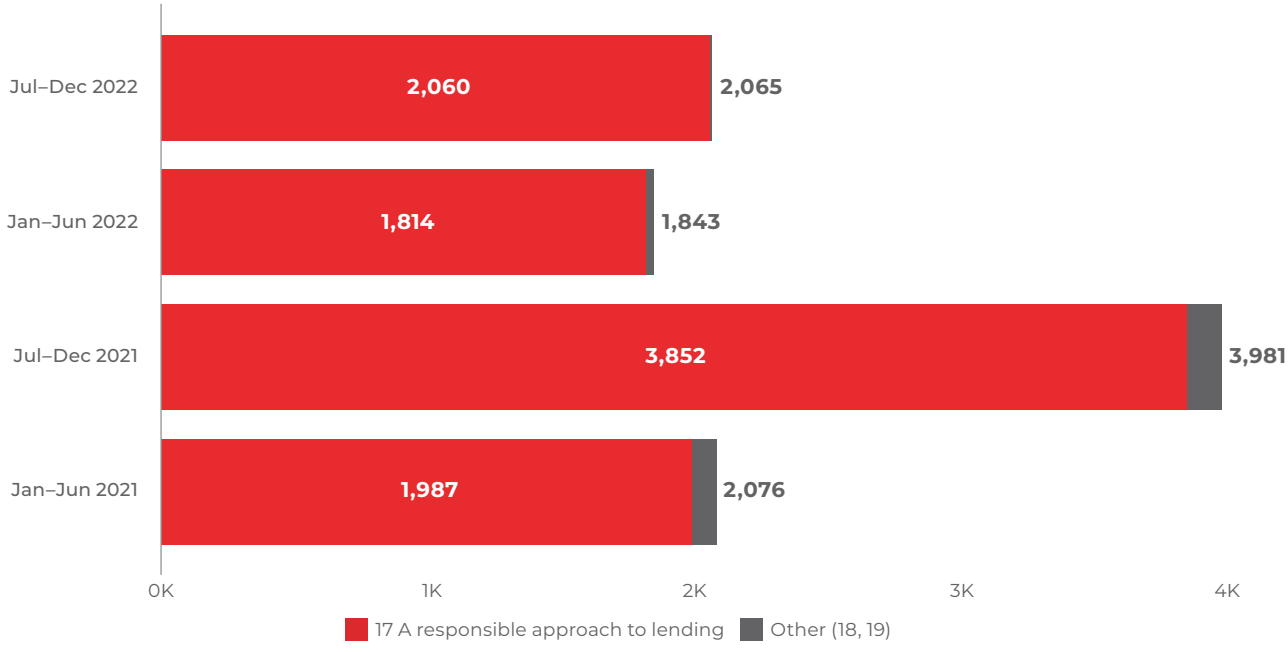


Chart 12: Breaches of Part 6 by Chapter

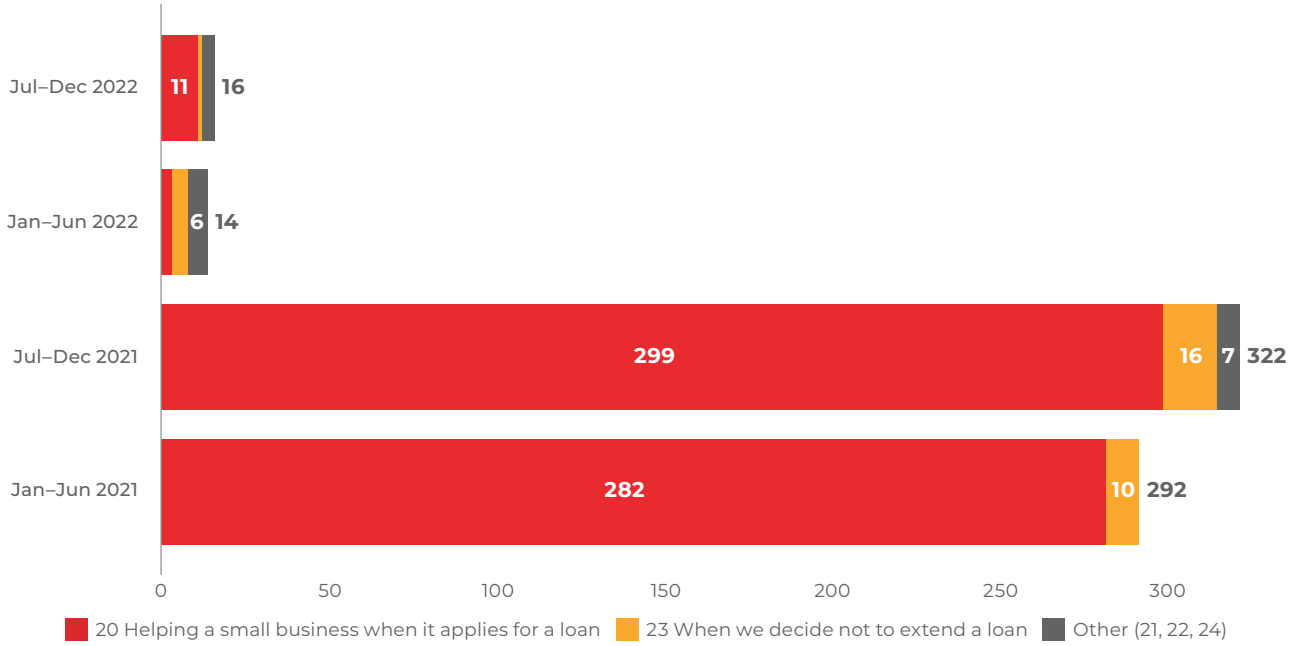


Chart 13: Breaches of Part 7 by Chapter

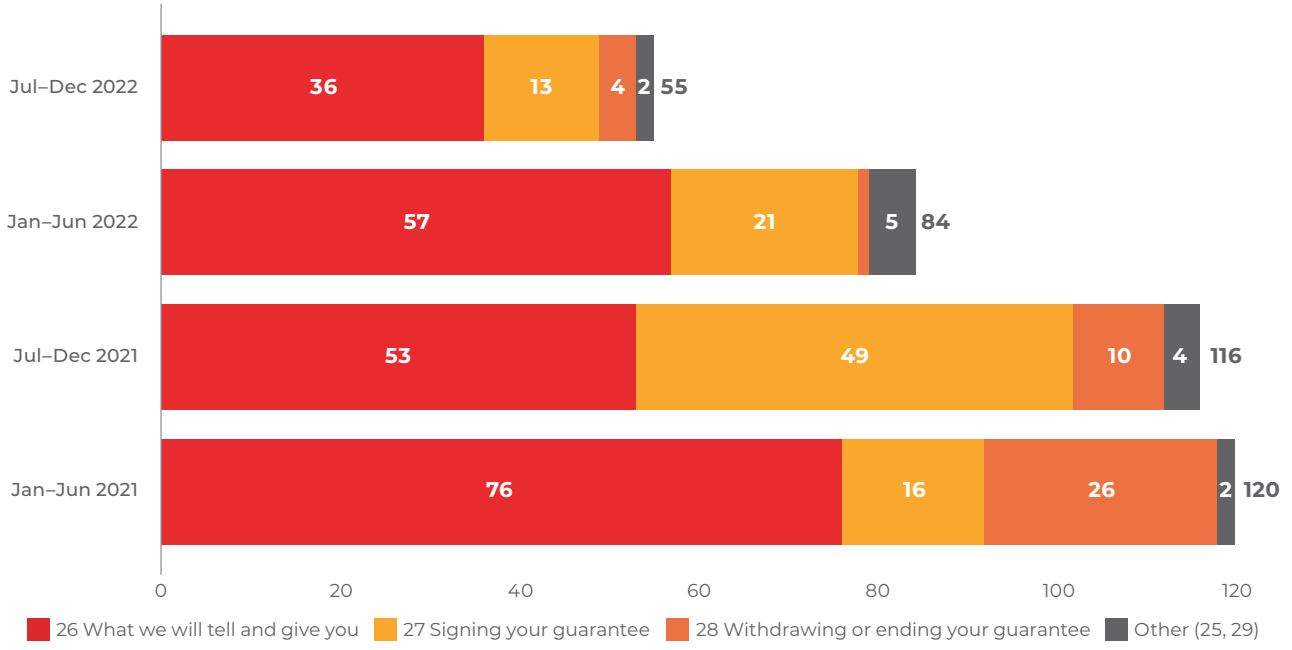


Chart 14: Breaches of Part 8 by Chapter

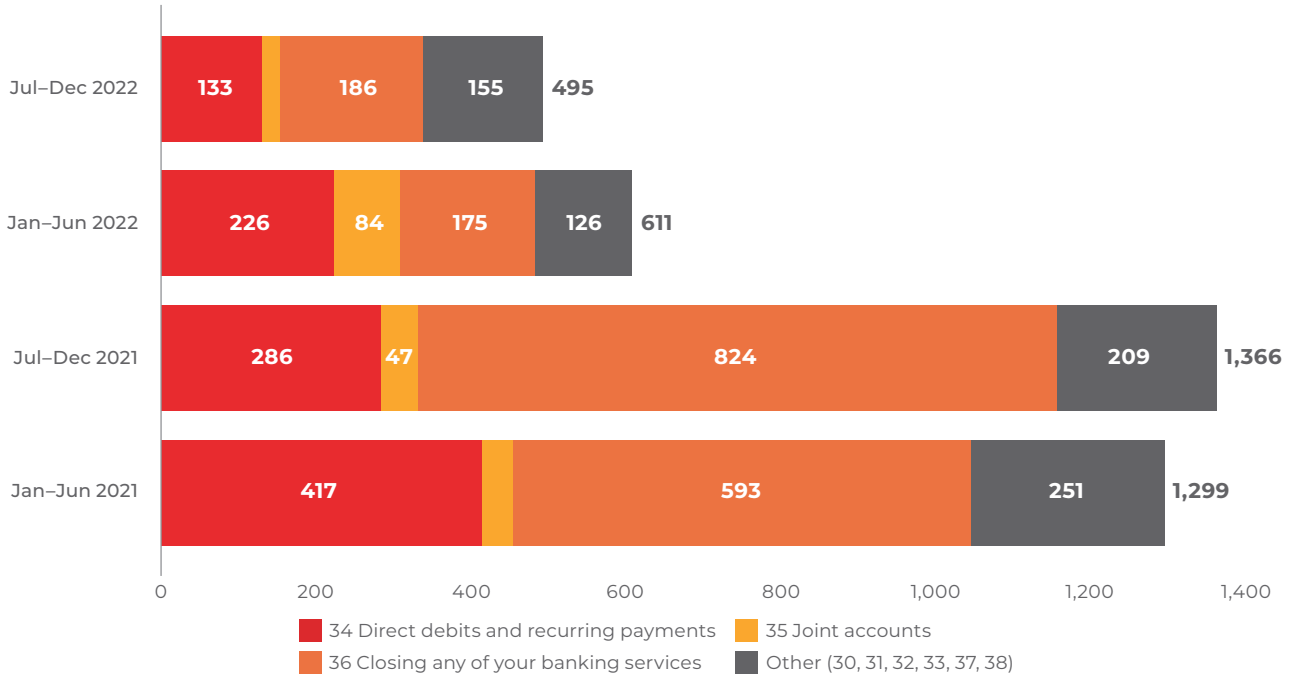


Chart 15: Breaches of Part 9 by Chapter

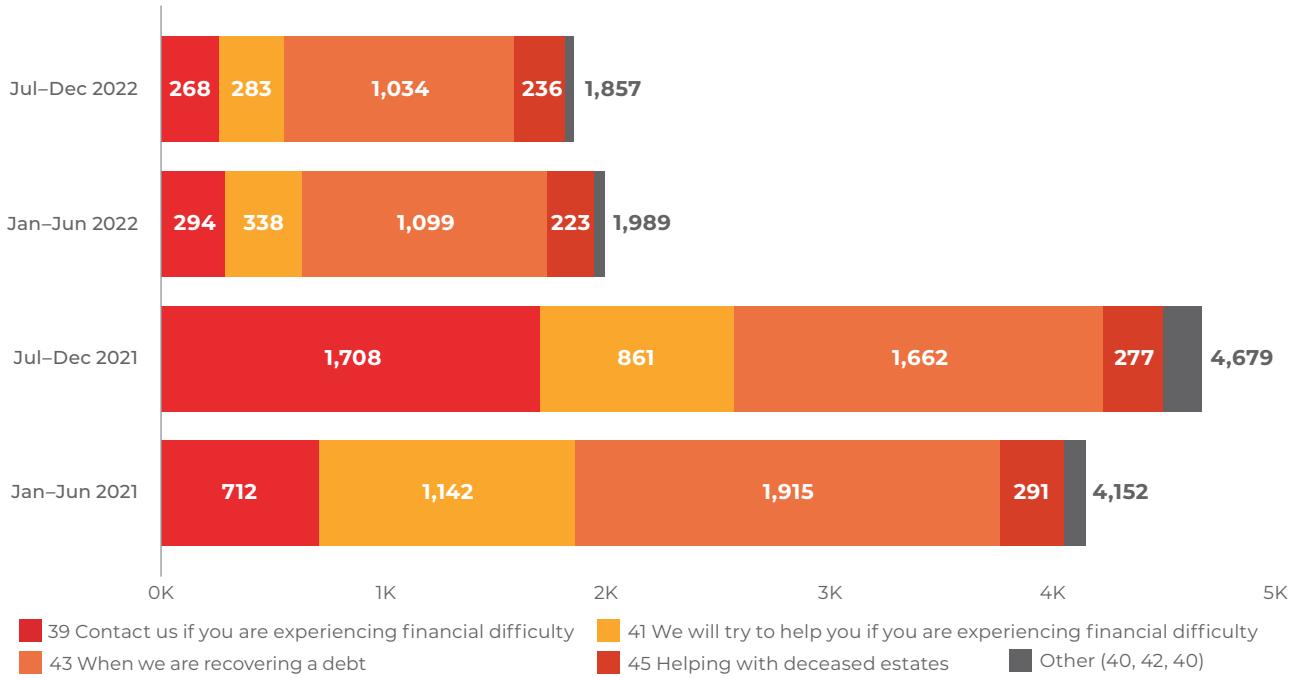
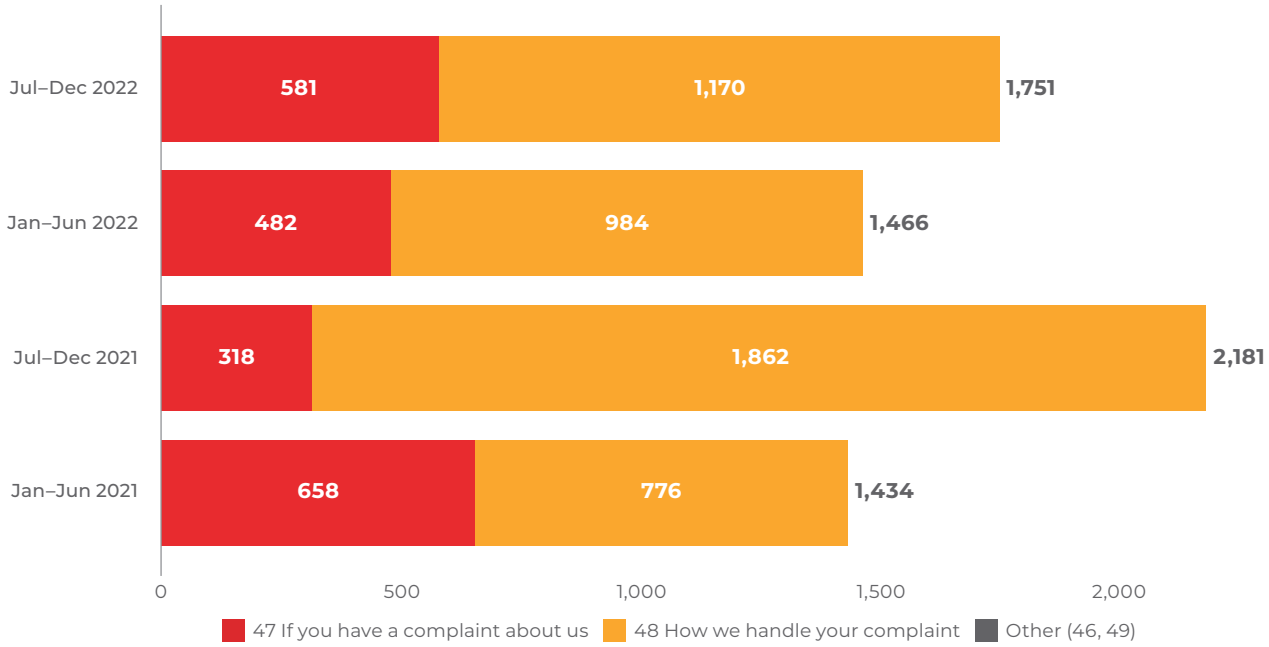


Chart 16: Breaches of Part 10 by Chapter



Comparing 2021 and 2022

2021		2022
15,861 (35%) of total breaches analysed		**13,676 (45%)** of total breaches analysed
Top causes of breaches		
78%	Human error	80%
15%	Deficiency in process or procedure	8%
5%	System error	5%
Top identification method of breaches		
52%	Line 1 monitoring	39%
21%	Customer complaint	35%
20%	Self-reported by bank staff	19%
Top corrective actions taken		
65%	Staff training	70%
4%	Ongoing investigation	9%
19%	Process review or improvement	8%

Trained and competent staff (Chapter 4)			**Protecting confidentiality (Chapter 5)**		
2021		**2022**	**2021**		**2022**
5,228	Total breaches	5,063	9,011	Total breaches	7,477
45% (2,350)	Breaches analysed	58% (2,923)	28% (2,516)	Breaches analysed	28% (2,096)
2m	Customers affected	2.2m	4.2m	Customers affected	2.2m
$65.3m	Financial loss	$ 81.7m	$7.7m	Financial loss	$ 5.3m

Communication with customers (Chapter 9)			Inclusive and accessible banking (Chapter 13–16)		
2021		2022	2021		2022
3,128	Total breaches	2,354	1,900	Total breaches	1,014
30% (945)	Breaches analysed	52% (1,232)	18% (337)	Breaches analysed	32% (324)
9.1m	Customers affected	8.5m	51,754	Customers affected	11,525
$19.9m	Financial loss	$26.1m	$7.35m	Financial loss	$10.8m

Responsible lending (Chapter 17)			Financial difficulty (Chapter 39–41)		
2021		2022	2021		2022
5,839	Total breaches	3,874	4,463	Total breaches	1,205
24% (1,422)	Breaches analysed	58% (2,250)	43% (1,928)	Breaches analysed	54% (649)
24,822	Customers affected	56,109	24,124	Customers affected	38,773
$25.6m	Financial loss	$15.8m	$341,014	Financial loss	$3m

Debt recovery (Chapter 43)			Complaint handling (Chapter 47–48)		
2021		2022	2021		2022
3,577	Total breaches	2,133	3,614	Total breaches	3,217
57% (2,041)	Breaches analysed	53% (1,130)	26% (939)	Breaches analysed	39% (1,250)
112,710	Customers affected	1.4m	11,496	Customers affected	21,360
$6m	Financial loss	$1.4m	$818,588	Financial loss	$354,467

About us

We are an independent monitoring body established under paragraph 207 of the Code. Our purpose is to monitor and drive best practice Code compliance.

To do this, we:

- examine the practices of banks
- identify current and emerging industry wide problems
- recommend improvements to bank practices
- sanction banks for serious compliance failures
- consult and keep stakeholders and the public informed.

Our 2021–24 Strategic Plan sets out our overall objectives to fulfil our purpose to monitor and drive best practice Code compliance. Our 2023–24 Business Plan sets out the priority areas and activities we will undertake to meet the objectives in the Strategic Plan.

See more information about us and members of the Committee.

The Banking Code Compliance Statement

We developed the Compliance Statement to collect data from banks about breaches. The Compliance Statement program is conducted in accordance with clause 4.2 of our Charter.

It enables us to:

- benchmark compliance with the Code
- report on current and emerging issues in Code compliance to the industry and the community
- establish the areas of highest priority for future monitoring.

Banks are required to provide breach data twice a year for the preceding six-month reporting period. They are required to report the total number of breaches they identified during the reporting period, and more details for each breach that meets any of the following criteria:

- the breach of the Code was considered to be significant, systemic or serious by the bank or any other forum
- the breach affected more than one customer
- the breach had a financial impact of more than $1,000 on a customer
- the nature, cause and outcome of more than one breach are the same.

In addition, banks are required to report details for a random sample of 5% of the remaining breaches of each Code Chapter.

‘Three lines of defence’

In this report, we have referred to a model of monitoring commonly used by banks called the ‘three lines of defence’. This refers to the three ‘lines’ within a business unit responsible for addressing compliance risk.

While the model is applied in different ways, generally it features:

- The first line – business units which own the compliance risks and have day-to-day responsibility for breach prevention and compliance monitoring
- The second line – the specialist function that develops risk management policies, systems and processes
- The third line – internal audit with responsibility for reviewing the effectiveness of the compliance framework and independently reporting to the Board.

More about the ‘three lines of defence’ model is provided by the Australian Prudential Regulation Authority.