BCCC
Banking Code
Compliance Committee

Compliance with the **Banking Code of Practice**

January to June 2023

Contents

Chair's message

It is important to start with a notable achievement — an overall 9% decrease in breaches, including decreases for three of the major banks, during this reporting period.

It signifies a concerted effort by the banking sector to improve practices and uphold the standards in the Code.

However, our optimism is tempered by a concerning increase in breaches of Part 9 of the Code, which contains the crucial obligations to support customers facing financial difficulty. The almost 40% increase of these breaches is alarming.

In a time marked by escalating inflation and living costs, the imperative for banks to provide support to customers in financial difficulty cannot be overstated. Breaches of these obligations can lead to serious consumer detriment.

Banks reported failing to respond to financial hardship requests, persisting with debt collection activities despite hardship arrangements being in place, and neglecting to follow through on agreed-upon hardship arrangements. Such failings not only breach Code obligations, but they also contribute to a decline in trust and confidence in the industry.

Banks have had ample time to anticipate the surge in financial hardship requests and implement measures to manage them effectively. As we move into the next reporting period, we expect the industry to prioritise improvements in staff training, systems and procedures to better support people in need during these challenging times.

Our report highlights another emerging concern—a suspected underreporting of breaches.

Underreporting of breaches signals risks with inadequate processes and systems or lack of commitment to Code obligations. Ultimately, this undermines banks' ability to identify and correct issues and improve customer outcomes, which in turn jeopardises the efficacy and benefits of the self-regulatory Code.

We will continue to monitor the progress and outcomes of the industry's response to these challenges. We know that banks have a range of ways to support customers experiencing financial difficulty. They need to do more to provide that support fairly and consistently.

We look forward to working with banks to strengthen compliance with the Code through better reporting and safeguard the trust that is at the core of the industry's relationship with customers.

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 for the preceding six-month period.

This report summarises the data for the period of January–June 2023.

As well as reporting the total number of breaches they identified during the reporting period, banks must provide more details for a sample of incidents that meet certain criteria.

The details for this sample include information about the nature, cause, impact of the breaches, and how the bank corrected them.

For January–June 2023, from a total 14,165 breaches, banks provided more details for 6,100 breaches.

Note: The 'financial impact' we cite throughout this report refers to the actual or estimated financial impact on the customer or the bank at the time of reporting. In most cases, the numbers of customers affected we cite are rounded.

Snapshot

January to June 2023

Breaches down 9%. This follows a 3% increase in the last reporting period.

Lowest number of breaches reported since the inception of the BCCC.

Chart 1: Trend in total breaches

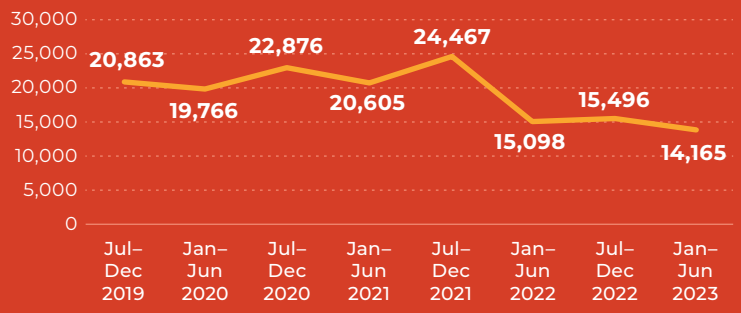
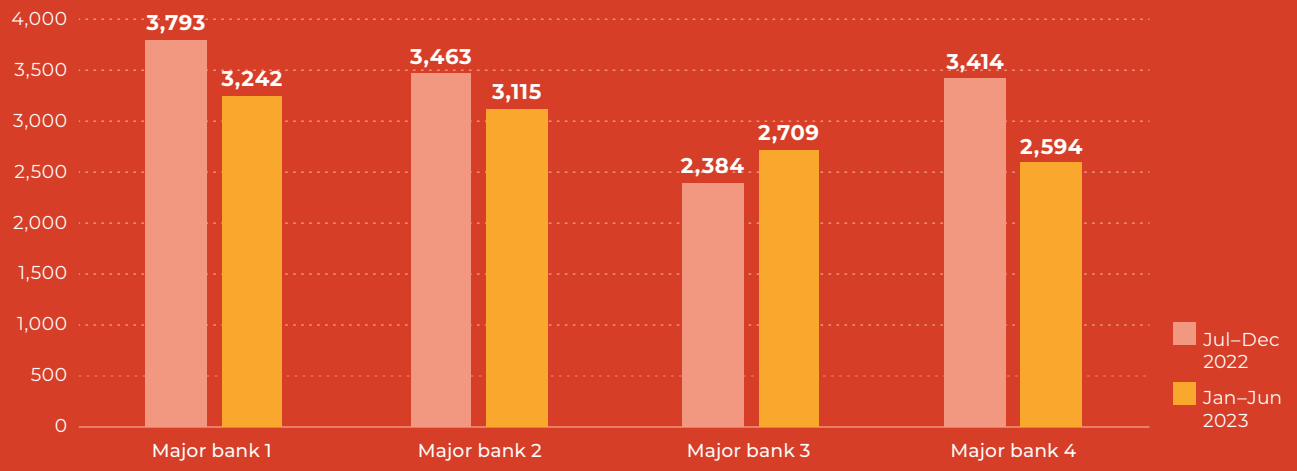


Chart 2: Breaches by the four major banks



The **four major banks** accounted for **82% (11,660) of the breaches** reported in this period (down from 84% in the last reporting period).

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

Nine of the 13 non-major banks reported an **increase in breaches**.

Nine banks (including three major banks) **reported increases** in Part 9 When things go wrong, contributing to an overall 39% increase in Part 9.

$46.4 million financial impact down from $56.2 million in the last period.

4.5 million affected customers down from 9 million in the last period.

Based on a sample of 6,100 breaches (compared to a sample of 6,193 breaches used in the last period).

Table 1: Most breaches by Code Part

Code Part		Jan–Jun 2023		Jul–Dec 2022	
		Breaches	Change	Breaches	Change
Pt 02	Your banking relationship	5,328	↓ 17%	6,423	↑ 5%
Pt 09	When things go wrong	2,588	↑ 39%	1,857	↓ 7%
Pt 03	Opening an account and using our banking services	2,108	↓ 11%	2,366	↓ 2%
Pt 05	When you apply for a loan	1,737	↓ 16%	2,065	↑ 12%
Pt 10	Resolving your complaint	1,401	↓ 20%	1,751	↑ 19%
Pt 08	Managing your account	499	↑ 1%	495	↓ 19%
Pt 04	Inclusive and accessible banking	444	↓ 5%	468	↓ 14%
Pt 07	Guaranteeing a loan	47	↓ 15%	55	↓ 35%
Pt 06	Lending to small business	13	↓ 19%	16	↑ 14%
Pt 01	How the Code works	0	0%	0	0%
Total		**14,165**	**↓ 9%**	**15,496**	**↑ 3%**

Note: The column showing breaches in Jul–Dec 2022 was corrected on 15 December 2023.

Table 2: Top 5 Code Chapters with the most breaches

Code Chapter		Breaches	Change from previous period
Ch 05	Protecting confidentiality	3,251	↓ 18%
Ch 04	Trained and competent staff	2,072	↓ 15%
Ch 17	A responsible lending approach	1,727	↓ 16%
Ch 43	When we are recovering a debt	1,303	↑ 26%
Ch 48	How we handle your complaint	1,292	↑ 10%

Table 3: Notable increases in breaches by Code Chapter

Code Chapter		Breaches	Change from previous period
Ch 10	Responding to your request for information	53	↑ 231%
Ch 45	Helping with deceased estates	477	↑ 102%
Ch 41	We will try to help you if you are experiencing financial difficulty	422	↑ 49%
Ch 43	When we are recovering a debt	1,303	↑ 26%
Ch 39	Contact us if you are experiencing financial difficulty	326	↑ 22%

Table 4: Notable decreases in breaches by Code Chapter

Code Chapter		Breaches	Change from previous period
Ch 47	If you have a complaint about us	109	↓ 81%
Ch 08	Providing you with information	485	↓ 26%
Ch 05	Protecting confidentiality	3,251	↓ 18%
Ch 17	Responsible approach to lending	1,727	↓ 16%
Ch 04	Trained and competent staff	2,072	↓ 15%

General findings

We use the data we collect to evaluate industry-wide issues and trends, providing a unique overview of the banking sector.

It also allows us to provide banks with individual benchmark reports, which track their compliance performances and offer insightful comparisons with peers.

When the data indicates concerns, we engage with banks on the issues and work to ensure they address breaches and mitigate risks of further non-compliance.

Cause of breaches

The top three causes of reported breaches were human error, deficiency in process or procedure and system error or failure. These three causes account for 94% of all breaches.

Banks attributed 4,970 breaches (81%) to human error in the breach sample for January to June 2023. Of these 4,970 breaches, banks only identified another root cause for 32 (0.6%).

We reiterate our message that all banks must strengthen their efforts to identify and address the root causes of recurring breaches.

As Chart 3 shows, at the industry level, there has been no shift in the top three causes of breaches in the last three reporting periods.

While human error remains the main cause of breaches across the industry, there is a significant variation in the proportion of breaches caused by human error among individual banks. For the major banks, the proportions range from 70% to 92%.

Chart 3: Top 3 causes of breaches

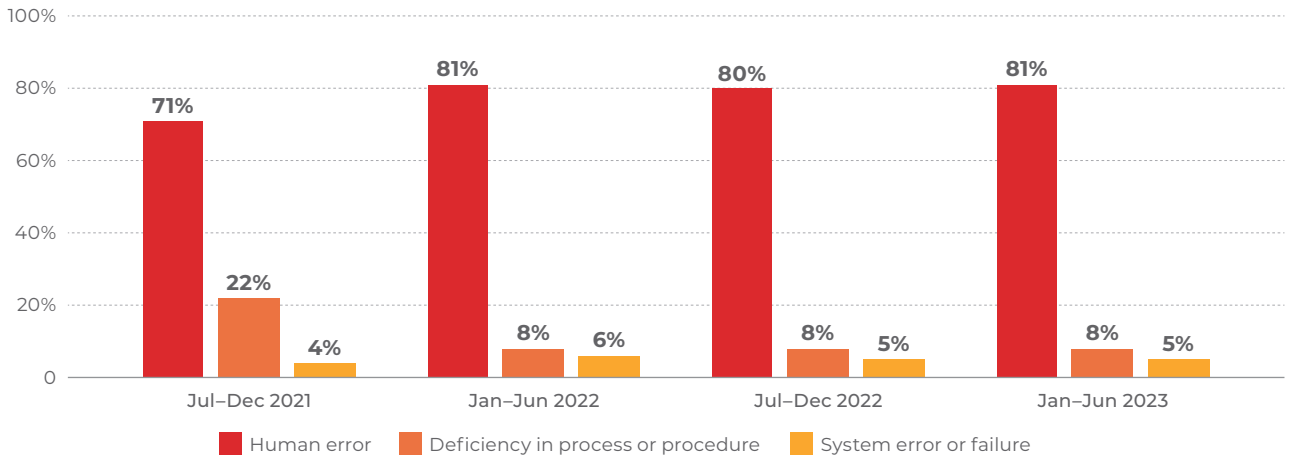


Table 5: Top 3 causes of breaches Jan–June 2023

Banks	Cause of breach	Breaches %	Customers impacted	Financial impact
Major Banks	Human error	83%	1.34 m	$13.76 m
	Deficiency in process or procedure	7%	1.22 m	$17.12 m
	System error or failure	5%	1.74 m	$5.23 m
Non-major Banks	Human error	74%	73,000	$3.08 m
	Deficiency in process or procedure	11%	49,000	$3.03 m
	Insufficient training	5%	800	$217,000

Identifying breaches

Improving by 3% on the previous period, banks identified 50% of reported breaches through Line 1 monitoring and quality assurance processes.

While Line 1 monitoring processes and staff identification should be the primary method for identifying Code breaches, we continue to encourage banks to use a range of methods to identify breaches.

Five of the 17 banks identified more than 50% of their breaches through customer complaints. We encourage these banks to focus on identifying breaches through proactive methods, including Line 1 monitoring processes and staff identification.

Chart 4: Top 3 methods for identifying breaches

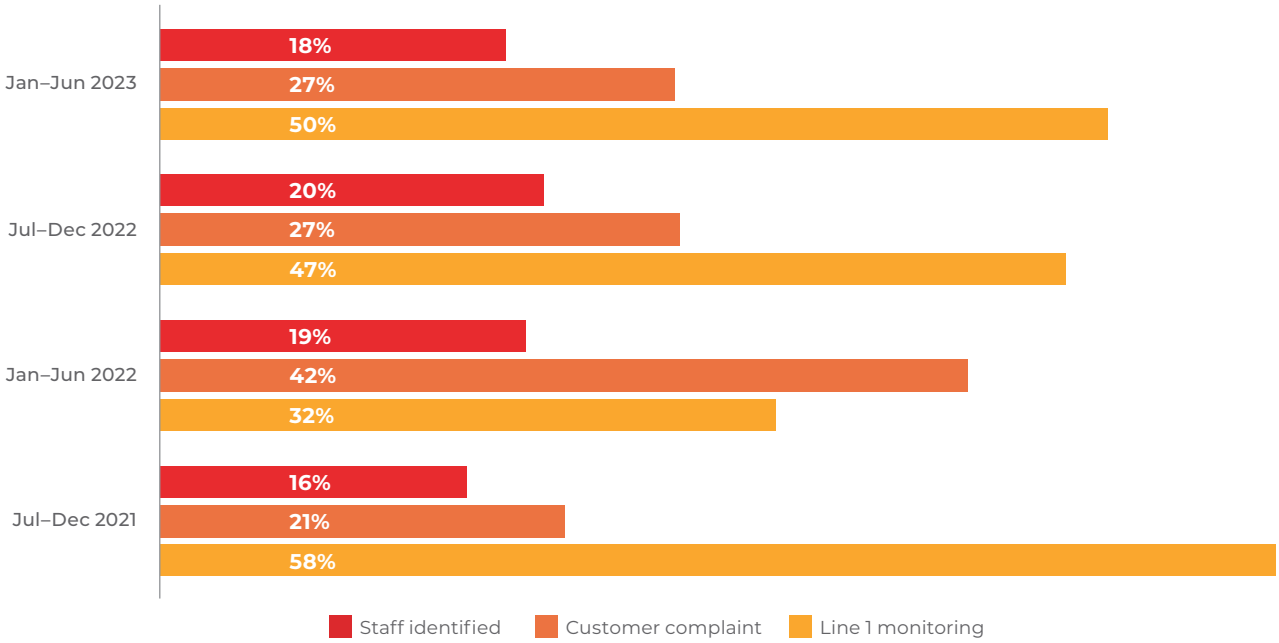


Table 6: Top 3 methods for identifying breaches Jan–June 2023

Banks	Breach identification method	Breaches %	Customers impacted	Financial impact
Major Banks	Line 1 monitoring	57%	499,000	$5.91 m
	Customer complaint	22%	510,000	$10.26 m
	Staff identified	16%	2.15 m	$22.85 m
Non-major Banks	Customer complaint	45%	59,000	$4.07 m
	Staff identified	25%	68,000	$705,000
	Line 1 monitoring	23%	59,000	$463,000

Impact of breaches

The sample breaches affected 4.5 million customers, approximately half the number of customers affected in the sample in the previous reporting period.

Consequently, the financial impact of these breaches decreased by $9.8 million.

Top three breaches by number of affected customers:

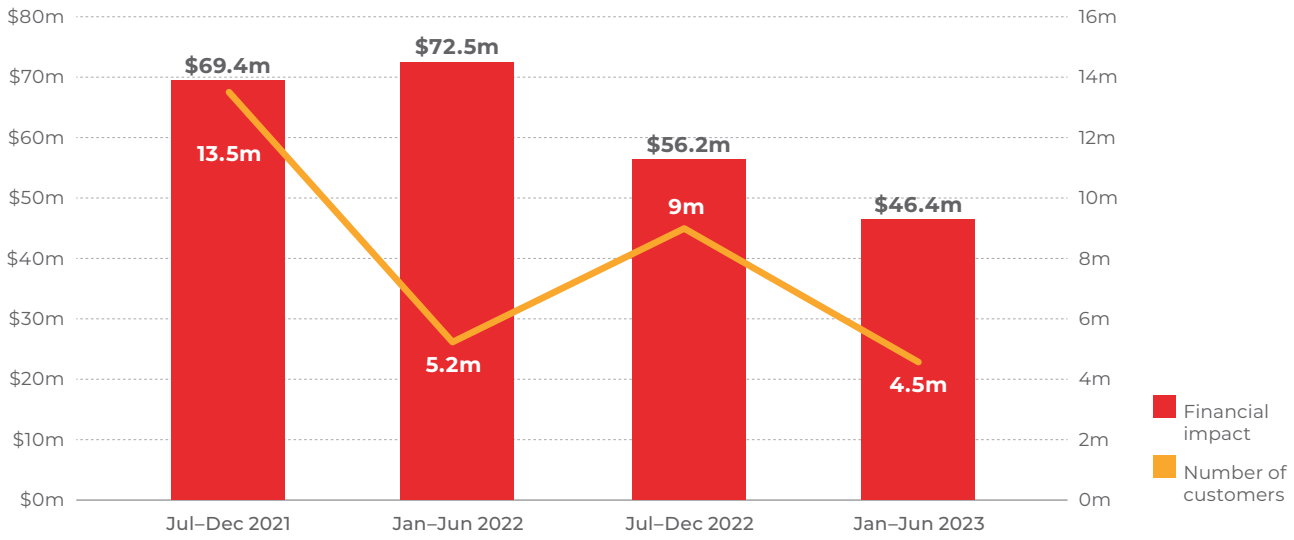
- One major bank sent inaccurate information about rewards points to its customers through a communication platform owned by a third party. This was a breach of Chapter 8 (Providing you with information) and Chapter 9 (Communication between us and you). The breach affected **627,000** customers and the bank attributed it to human error.
- One major bank sent communications to customers on their non-preferred channels. This was reported by the bank as a breach of Chapter 4 (Trained and competent staff), which includes the obligation to engage with customers in a fair, reasonable and ethical manner. The breach affected approximately **586,000** customers and the bank attributed it to an internal system error.
- One major bank failed to send email notifications to inform customers that their statements were accessible online. This was a breach of Chapter 31 (Statements we will send to you). The breach affected **512,000** customers and the bank attributed it to an internal system error.

Top three breaches by financial impact:

- One major bank set up repayments incorrectly for loans it had approved. This had a financial impact of **$12 million**, and the bank is still investigating the number of affected customers.
- One major bank charged additional interest on home loans due to missing offset account data. This had a financial impact of **$2.3 million** and affected 262,600 customers.
- One major bank reported that additional cardholders were incorrectly allowed to spend on customer accounts after being removed as additional cardholders. This had a financial impact of **$2.1 million** and affected 18,600 customers.

These were all reported as breaches of Chapter 4 (Trained and competent staff).

Chart 5: Impact of breaches



Corrective action

Corrective action is designed to address the root cause of the breach, prevent the breach from reoccurring and deliver positive outcomes for customers.

Staff training continues to be reported as the primary corrective action to prevent future breaches.

While this will always be an important form of corrective action, it is crucial that banks also get processes right to support staff and minimise the risk of breaches.

We encourage an increased focus on improvements in processes, systems and controls to identify and address deeper issues.

Chart 6: Corrective actions taken in response to breaches

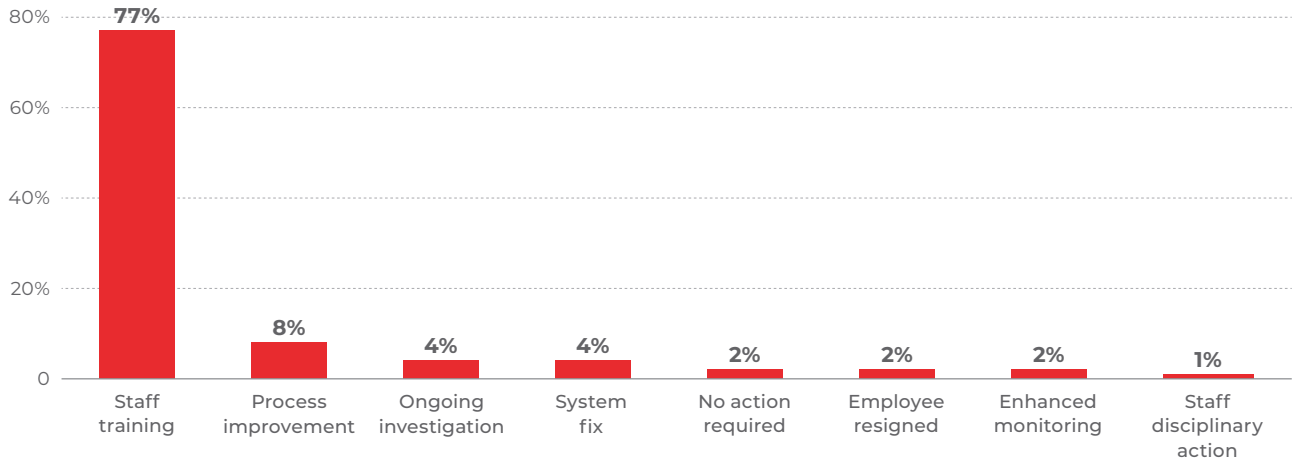


Table 7: Most common corrective action taken by banks Jan–June 2023

Banks	Corrective action	Breaches %	Customers impacted	Financial impact
Major Banks	Staff training	79%	377,000	$23.73 m
	Process improvement	7%	1.35 m	$5.71 m
	System fix	4%	1.31 m	$4.33 m
Non-major Banks	Staff training	71%	13,000	$2.88 m
	Process improvement	13%	48,000	$1.02 m
	Enhanced monitoring	4%	40,000	$51,000
	System fix	4%	77,000	$801,000

Remediating breaches

We analyse remediation data to understand how banks responded to the customer impact of breaches and provide key insights on the type of responses employed.

Banks reported a total financial impact of $33.1 million where they made remediation payments during the reporting period, with major banks accounting for 89% of this financial impact ($29.45 million).

However, the predominant form of remediation was communication with the customer. Between January and June 2023, over 2 million customers affected by breaches (46%) were sent communication as remediation.

Banks reported that 21% of breaches, affecting over 323,600 customers, required no remediation. Of these breaches, the ones that affected the highest number of customers related to breaches from incorrect information on the banks' websites.

The proportion of remediation methods employed differed across the major banks.

Most common remediation method for each of the four major banks:

Major bank 1: No customer remediation required (23%)

Major bank 2: Communication with customer (29%)

Major bank 3: No customer remediation required (45%)

Major bank 4: Customer refund/reimbursement/goodwill (37%)

In some cases, banks reported no remediation for breaches that we would generally see remediation to include a financial component. For example:

- One bank did not provide a customer with $2,000 they were entitled to through a cash-back offer after a home loan settlement. The bank reported that no customer remediation was required.
- A customer expressed concerns that their online banking account may have been compromised. The employee did not block the customer's internet banking despite it being part of the bank's procedure. The customer later confirmed that money had been taken out of the account. The bank reported that no customer remediation was required.

It is important banks report this information accurately for us to report on how banks manage the impacts of breaches on customers.

Chart 7: Remediating breaches

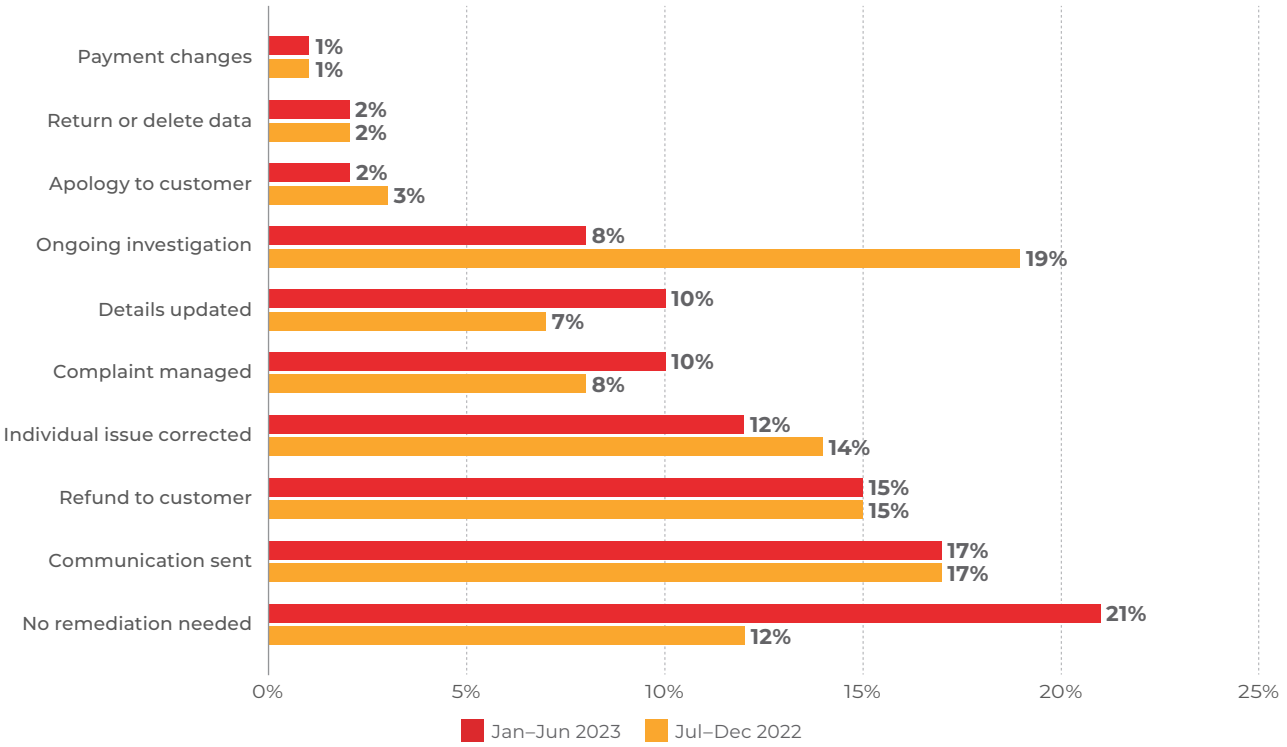


Table 8: Top 3 ways banks remediated customers Jan–June 2023

Category of bank	Remediation method	Breaches %	Customers impacted	Financial impact
Major Banks	No remediation needed	25%	304,000	$249,000
	Communication sent	17%	1.98 m	$1.69 m
	Refund to customer	15%	310,000	$29.45 m
Non-major Banks	Communication sent	20%	124,000	$364,000
	Complaint managed	17%	1,000	$316,000
	Individual issue corrected	17%	9,000	$408,000

Key observations

When things go wrong

In the current economic climate, more people are facing financial challenges and turning to their bank for guidance and assistance. In fact, with support of the ABA, banks have been encouraging customers to engage early when faced with financial difficulty.

Failing to support customers experiencing financial difficulty can lead to unmanageable debt, delayed recovery from financial strain and emotional stress.

We are concerned by a significant increase in the number of overall breaches of the Code obligations that relate to supporting customers in financial difficulty. We saw the greatest increases in breaches of Part 9, Chapters 39, 41, 42 and 43.

Banks must do more to comply with obligations in the Code to support customers who are experiencing financial difficulty.

As banks expand their teams for dealing with financial difficulty in response to customer needs, new staff must be supported with comprehensive training programs that accelerate their speed to competency.

As part of this, we encourage banks to develop targeted training for breach reporting. This should focus on risk awareness across the bank and improving breach identification and reporting by frontline staff.

Currently, ASIC is conducting a review of practices that address financial hardship, and this will place banks under scrutiny. The review is a priority for ASIC, which has clearly set out its expectations of lenders, and has direct relevance to Code obligations. We will monitor the progress and outcome of this work closely.

While not cited as a reason for the increase in breaches, ASIC's work may have affected the results by focusing the attention of banks on their support for customers facing financial difficulty.

We stress the importance of proactively reviewing processes, procedures and quality assurance in critical areas of operations. Waiting until the scrutiny of third parties before acting is not good enough.

With the number of Australians experiencing financial hardship expected to increase, complying with Code obligations for financial difficulty is more important than ever.

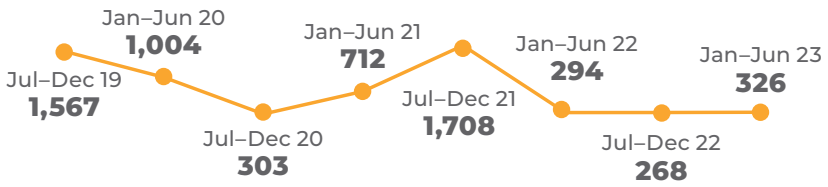
We urge banks to consider the findings in our report and take appropriate action to ensure they mitigate compliance risks.

Part 9, Chapter 39: Contact us if you are experiencing financial difficulty

Up by

22%

(↑58 breaches)



Banks reported a 22% increase in Chapter 39 breaches. This followed decreases in the two preceding reporting periods.

Chapter 39 of the Code sets out obligations for banks to assist customers facing financial difficulty. When contacted by customers facing financial difficulty, a bank must explore available options and provide the customer (or their financial counsellor or representative) with information about the ways the bank can help.

Of the 326 breaches of Chapter 39, the major banks reported 304 (93%).

In the sample data, the most common breaches of Chapter 39 included:

- Failing to promptly respond to a hardship request.
- Failing to deal with a third-party representative as requested by the customer.

When a bank fails to identify or respond to a request for support, it can lead to the customer falling deeper into hardship, making it more difficult to recover in the longer term.

Too often banks did not promptly respond to hardship requests, resulting in a range of financial impacts.

All banks must have sufficient processes in place to ensure a prompt response to every request for support, especially in the current economic climate. Unlike the COVID-19 pandemic, there has been more time to prepare for this and be better equipped to manage the increased demand.

We are also concerned with the number of breaches relating to banks not following a customer's instruction to deal with their financial counsellor or third-party representative.

Complying with this obligation is vital for customers, and banks must improve. We know that customers who use a financial counsellor or third-party representative are more likely to be experiencing financial hardship or vulnerability. Not following a customer's instructions may cause unnecessary and avoidable stress.

We will follow up on this issue in the coming year.

Breach sample

The breach sample provided more detailed information for 244 breaches. These breaches affected 12,000 customers and had a financial impact of $184,000.

Examples of breaches

- One major bank failed to promptly respond to financial hardship enquiries from seven customers which resulted in a total financial impact of $63,727.
- One major bank failed to deal with a customer's financial representative, as requested by the customer. This resulted in a financial impact of $13,935.
- One major bank failed to respond to a customer's request for financial hardship assistance within the required timeframe. This affected the customer's comprehensive credit report and resulted in a financial impact of $5,508.

Case study

Of all the breaches of Chapter 39 by the major banks, one major bank accounted for 82% (201 of 244).

Its breaches had a financial impact of $55,803 and affected 317 customers.

The bank attributed the cause of these breaches to the complex and technical nature of managing financial difficulty and a reliance on manual processes. The bank also cited an increase in financial hardship applications as a contributing factor.

In response the bank has:

- added more staff and focused on staff training and improving procedures to reduce breaches
- planned to include vulnerability identification by frontline staff in performance scorecards, and
- planned to rescope its National Credit Code action plan to simplify manual processes.

The bank reported it corrected 13% of the breaches through process reviews and improvements, and only 1% through system fixes or improvements.

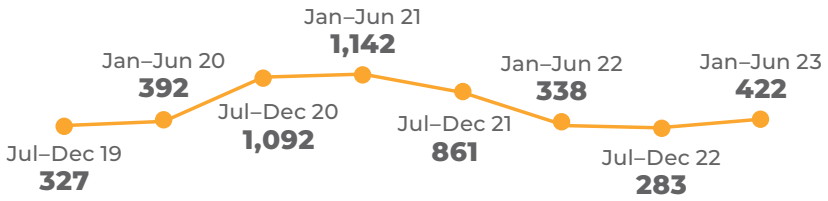
This bank's number of breaches of this Chapter is out of step with its peers, and we expect it to review its processes and systems to reduce recurrence of these breaches.

Part 9, Chapter 41: We will try to help you if you are experiencing financial difficulty

Up by

49%

(↑139 breaches)



Banks reported a 49% increase in breaches of Chapter 41 obligations.

For the three previous reporting periods, breaches of Chapter 41 obligations had been trending down.

The obligations in Chapter 41 set out the commitments for banks to provide support when customers face financial difficulty. A bank must work with individual customers and consider their unique financial situation when offering information, support or referral to a financial counselling organisation.

Of the 422 breaches of Chapter 41, the major banks reported 95% (400).

In the sample data, the most common breach was failing to offer or provide financial hardship assistance despite receiving a notification or trigger that a customer may require support.

Supporting customers facing financial difficulty is a fundamental aspect of the Chapter 41 obligations. Every bank must get this right.

Most breaches of the obligations in Chapter 41 were caused by human error (85%). It is important that banks analyse these breaches to understand their root causes and how best to address them promptly.

Banks should consider measures to ensure their staff are adequately prepared to handle financial hardship queries and are aware of their Code obligations.

Breach sample

The breach sample provided more detailed information for 100 breaches. These breaches affected 1,000 customers and had a financial impact of $355,000.

Examples of breaches

- One major bank mismanaged a hardship request it received in 2019. The mismanagement was exacerbated with multiple case managers over a four-year period due to staff attrition. It resulted in over $245,531 in financial impact.
- One major bank failed to provide financial hardship assistance to a customer in response to a hardship trigger. It did not provide useful and clear information about arrears and did not establish a direct loan repayment correctly. The failure resulted in further arrears for the customer and affected their repayment history. The breach had a financial impact of $11,040.
- One major bank reported several breaches in which it failed to put hardship arrangements in place for customers. This included failing to implement 0% interest on a customer's account and failing to implement 3 months' grace on repayments. This had a total financial impact of $15,825.

Case study

Of the 400 breaches of Chapter 41 obligations reported by major banks, one major bank was responsible for 44% (175 of 400).

This bank also attributed 90% of its sample breaches to human error. It cited staff training, coaching or feedback as the corrective action in 90% of the breaches.

The bank had recently onboarded many customer service staff in response to an increase in customer queries about financial hardship.

Despite the newer staff members undergoing intensive training, they tended to make more mistakes than their more experienced colleagues, especially in the first three months of employment.

Bringing in new staff provided essential support, but the inexperience also presented risks. It is crucial that increases in staff levels need to be accompanied by comprehensive onboarding and training processes, as well as proper oversight.

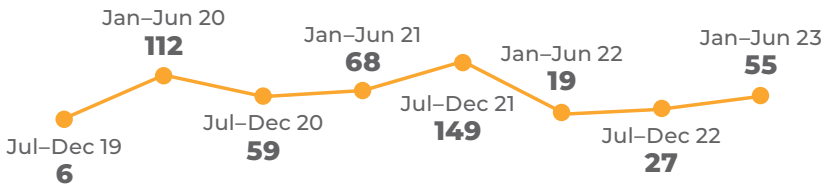
We expect to see future increases in customer service staff better support compliance with Chapter 41 obligations.

Part 9: Chapter 42: When you are in default

Up by

104%

(↑28 breaches)



Breaches of the obligation to inform customers when reporting their default activity to a credit reporting body more than doubled in the reporting period.

Banks commit to two obligations in Chapter 42:

- Informing customers when reporting their default activity to a credit reporting body.
- Not charging default interest or fees to farmers with loans for farming operations during droughts or natural disasters.

Three out of the four major banks accounted for 98% (54) of the breaches of the Chapter 42 obligations, while 12 out of the 13 non-major banks reported no breaches.

Most breaches related to failures to notify customers of default listings or errors in default listings. We are concerned about the rapid increase in breaches of this nature in a short time.

Informing customers about reported payment defaults is critical for transparency and fairness because it gives customers an opportunity to address any issues. For banks, this transparency is essential to maintaining trust with customers.

We encourage banks to review their current compliance frameworks to ensure they inform customers when reporting a default listing.

Breach sample

The breach sample provided more detailed information for 34 breaches. These breaches affected 155 customers and had a financial impact of $50,000.

Examples of breaches

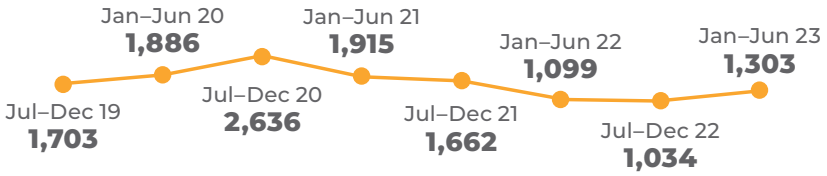
- One major bank reported that credit listing notification letters were not completed or sent to 95 home loan customers. The bank reported no financial impact.
- One major bank failed to notify a customer of a default prior to a default listing. The bank reported no financial impact.
- One bank reported that it made an incorrect default listing, affecting four customers. While the bank reported no financial impact, a breach of this nature can result in serious non-financial and financial detriment to the customer.

Part 9, Chapter 43: When we are recovering a debt

Up by

26%

(↑269 breaches)



Banks reported a total of 1,303 breaches of obligations in Chapter 43, a 26% increase on the previous reporting period. This is the first increase in breaches of Chapter 43 obligations we have seen in the last five reporting periods.

In Chapter 43, banks commit to clear guidelines for debt collection practices which require them to treat customers fairly and ensure the integrity of the debt recovery process.

In the sample data, the most common breaches of the obligations in Chapter 43 were:

- Carrying out debt collection activity when a hardship arrangement was in place.
- Selling debt when the bank was considering a customer's financial situation.
- Providing incorrect, incomplete or unclear information to a customer related to recovery of the customer's debt.

Banks attributed most Chapter 43 breaches to human error (87%).

We were encouraged to see that most breaches were identified through either Line 1 monitoring and quality assurance processes (78%)* or staff member reports (15%).

However, the consequences of these breaches can be severe, and banks need to do more to address the risk of breaches, particularly from human error.

As more customers approach their bank to seek hardship arrangements, preventing these breaches must be a strong focus in the period ahead.

Breach sample

The breach sample provided more detailed information for 789 breaches. These breaches affected almost 12,000 customers and had a financial impact of $286,000.

* Note: This percentage has been corrected from 75% to 78% on 15 December 2023.

Examples of breaches

- One major bank failed to implement a complaint resolution in a timely manner, and the debt collection activity continued after the agreement for a debt waiver. This resulted in a financial impact of $82,492.
- One major bank commenced a debt collection activity while a complaint was open. This resulted in a financial impact of $22,986.
- One major bank reported outbound contact with 506 customers who were on active payment arrangements. The bank reported no financial impact for this breach.
- One major bank sold debt to an external agency while the customer was complying with a payment arrangement. This resulted in financial impact of $1,500.

Case study

A major bank made contact with customers for debt collection activity when it should not have occurred.

In one incident, the bank carried out debt collection activity on accounts of 2,829 customers that had long-term payment arrangements in place.

In another incident, the bank sent default notices to 1,478 customers with personal loans during the hardship assistance 'hold period' on debt collection.

In a third incident, the bank contacted 454 customers for debt collection activity, despite these customers having hardship arrangements in place.

The bank reported no financial impact for these breaches, affecting over 4,700 customers.

The cause of these breaches was attributed in part to deficiency in process. We expect banks to have strong processes, systems and oversight arrangements in place to prevent issues of this nature. Debt collection must comply with obligations in the Code and should meet the expectations set out in the Debt Collection Guidelines (RG 96) from ASIC and the ACCC.

To improve, banks should:

- Review staff training and procedures periodically to ensure they conduct debt collection responsibly.
- Use and test monitoring controls to ensure that their debt collection complies with the Code and other regulatory obligations.

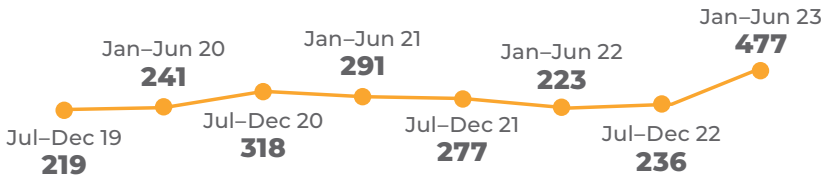
While the bank reported no financial impact for these breaches, they can have serious non-financial consequences. A customer may experience confusion, worry and stress if they receive new contact from the bank about their debt while they have hardship arrangements in place. The non-financial harm of breaches of this nature is an important element that banks cannot dismiss.

Part 9, Chapter 45: Helping with deceased estates

Up by

102%

(↑241 breaches)



Banks reported 477 breaches, the highest number for the past eight reporting periods and an increase of 102% since the last reporting period.

Banks have obligations under Chapter 45 to support customers in managing deceased estates. They must treat the deceased person's representative with respect and compassion, identify and stop charging relevant fees, and provide clear and accessible information on managing the deceased customer's accounts.

Most of the sample breaches of Chapter 45 related to failure to:

- Act on requests within the required notification timeframe of 14 days
- Provide clear and accessible information to a deceased customer's representative
- Correctly register a notification that a customer has passed away

Banks attributed 85% of the sample breaches to human error (higher than the 81% of all sample breaches attributed to human error).

While the increase in Chapter 45 breaches is concerning, we note that the issues reported mirror those identified in our 2023 report More work to do: A BCCC report on the management of deceased estates (2023 Deceased Estates Report).

We published our Deceased Estates Report on 9 June 2023, immediately after the January–June 2023 reporting period.

The report looked at information provided by six banks (including the four major banks) between July 2019 and September 2022 and highlighted compliance issues across all obligations and set the expectation that all banks examine their practices.

The themes from this reporting period align with the findings of our inquiry, that banks have more work to do to achieve better outcomes for representatives of deceased customers.

The increase in breaches of Chapter 45 can be explained in part by the focus that our inquiry brought during the reporting period.

Improvements that banks made following the 2023 Deceased Estates Inquiry are also a contributing factor. For example, one-time issues with system upgrades that led to breaches are now rectified. Also improved controls have enabled better oversight of breaches.

We expect breaches to come down as banks implement the recommendations made in our 2023 Deceased Estates Report and address the underlying issues. We will be following up with banks on their progress in the next 12 months.

Breach sample

The breach sample provided more detailed information for 182 breaches. These breaches affected 7,000 customers and had a financial impact of $184,000.

Examples of breaches

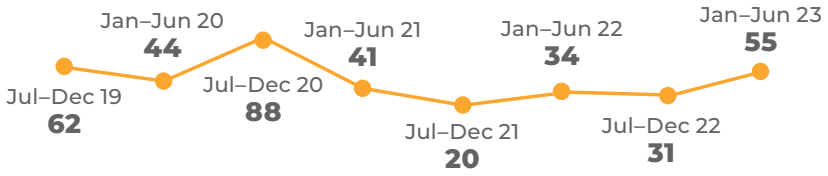
- One major bank reported a one-time operational issue with transition to an automated tool that resulted in a cohort of customers who did not have their requests processed within 14 days. This affected 3,245 customers.
- One major bank identified an automation system failure resulting in delays in meeting the 14-day timeframe to act on instructions for 468 deceased customers' accounts. The bank identified the incident through Line 1 monitoring or quality assurance processes, and corrected the issue through process review or improvement and staff training, coaching or feedback.
- One bank failed to register the notification that a customer had passed away and continued to charge account keeping fees totalling $30,630. The incident was caused by human error. The bank remediated the issue by reimbursing the funds and corrected it through staff training, coaching or feedback.

Part 8, Chapter 33: Managing a credit card or a debit card

Up by

77%

(↑24 breaches)



Banks reported an increase in breaches of Chapter 33 obligations relating to poor handling of disputed transactions on credit cards and debit cards.

In eight reporting periods, this is the third highest number of reported breaches of Chapter 33 obligations.

Chapter 33 sets out how banks will manage credit card and debit cards. This includes the commitments relating to increasing and decreasing credit card limits, disputing transactions, and providing notice of ending introductory offers.

In the sample data, the most common breaches of Chapter 33 obligations were:

- Failing to act on disputed transactions
- Delayed action on disputed transactions
- Not notifying customers that their introductory balance transfer offer on a credit card is ending

We urge banks to prioritise and enhance their efficiency in processing disputed transactions.

Scam threat

Scams are an ever-increasing threat and banks are responding to large numbers of disputed transactions.

Work must continue to ensure efficient processing of disputed transactions on credit cards and debit cards. This will maintain customer trust, mitigate financial losses and ensure compliance with regulations.

Swift resolution of disputed transactions helps minimise customer stress and financial impacts.

Breach sample

The breach sample provided more detailed information for 26 breaches. These breaches affected 3,000 customers and had a financial impact of $97,000.

Examples of breaches

- One major bank identified several breaches related to disputed transactions through its monthly quality assurance and monitoring. These breaches impacted 81 customers, but the bank reported no financial impact.
- One major bank failed to provide the required 30 days expiry notice to over 3,005 customers who had an introductory balance transfer on their credit card.
- One major bank reported that a failure to create a case in its system for a customer that fell victim to a bank impersonation scam resulted in $16,951 in financial impact.
- One major bank reported failing to act, or delaying action, on disputed transaction requests for seven customers. The total financial impact was $61,442, with one breach alone accounting for $15,180.

Spotlight

Underreporting of breaches

Consistently reporting no breaches or very few breaches over extended periods raises concerns that a bank does not take reporting seriously or does not have adequate systems in place to be able to identify breaches.

We have observed consistent reporting of no breaches or very few breaches by some banks over the last eight reporting periods in the following areas.

Ch 15 Banking services for customers on a low income

- Nine banks have not reported any breaches of Chapter 15 over the last eight reporting periods.

Ch 16 Basic accounts or low or no fee accounts*

- Eight banks have not reported any breaches of Chapter 16 over the last eight reporting periods.
- Four banks have reported fewer than six breaches of Chapter 16 over the last eight reporting periods.

*Currently, at least four banks offer basic accounts by default and would not be expected to report breaches of Chapter 16.

Part 6 Lending to small business

- Seven banks have not reported any breaches of Part 6 over the last eight reporting periods.
- Five banks, including one major bank, have reported five or fewer breaches over the last eight reporting periods.

Part 7 Guaranteeing a loan

- Four banks have not reported any breaches of Part 7 over the last eight reporting periods.
- Four banks have reported fewer than five breaches of Part 7 over the last eight reporting periods.

Ch 7 Closing a branch*

- Fourteen banks, including two major banks, have not reported any breaches of Chapter 7 over the last eight reporting periods.
- One major bank reported only two breaches of Chapter 7 over the last eight reporting periods.

*Currently, at least two non-major banks do not have branches and would not be expected to report breaches of Chapter 7.

The ABA Branch Closure Protocol (ABA Protocol) that was in effect up to 30 June 2023 applied to branch closures in inner regional, outer regional, remote and very remote Australia.[1]

Only three banks, including two major banks, have reported a total of 15 breaches of the ABA Protocol over eight reporting periods, from July 2019 to June 2023.

In APRA's report on deposit-taking institutions, it cited an 7% reduction in the number of bank branches (122 branches) across regional, remote and very remote Australia from June 2022 to June 2023.

Since the commencement of the Senate Inquiry into regional branch closures in February 2023, we understand three of the major banks have paused rural branch closures.

Nevertheless, the consistent reporting of no breaches or very few breaches of the ABA protocol, in an environment of branch closures, raises our concern that banks are not identifying and reporting breaches.

Risks of underreporting

Complying with the Code is crucial for delivering fair outcomes for customers and maintaining standards the community can trust. This extends to identifying and reporting of breaches.

We are concerned that low or no reporting could indicate a range of underlying issues with the compliance frameworks in place to identify breaches, such as:

- lack of staff awareness of Code obligations
- inadequate systems for accurately recording breaches
- inadequate monitoring and quality assurance.

The longer a breach remains undetected, the greater the risk of it developing into a serious and systemic issue. Once it reaches such a stage, the potential for detrimental effects on customers, as well as on the bank's operations and reputation, is significant.

Insufficient reporting presents a perception that the bank does not take its commitment to the Code seriously. This poses risks to the bank's reputation.

Transparent and accurate reporting is vital for upholding consumer protections and for maintaining the integrity of the banking industry.

We will continue to monitor risks of underreporting and will increase our scrutiny of the banks involved.

1. An updated ABA protocol came into effect on 1 July 2023. The requirements in the new Protocol are tiered, based on distance and all references to inner regional, outer regional, remote and very remote Australia have been removed.

Breach data

Breaches by Code Part and Chapter

Chart 8: Breaches of Part 2 by Chapter

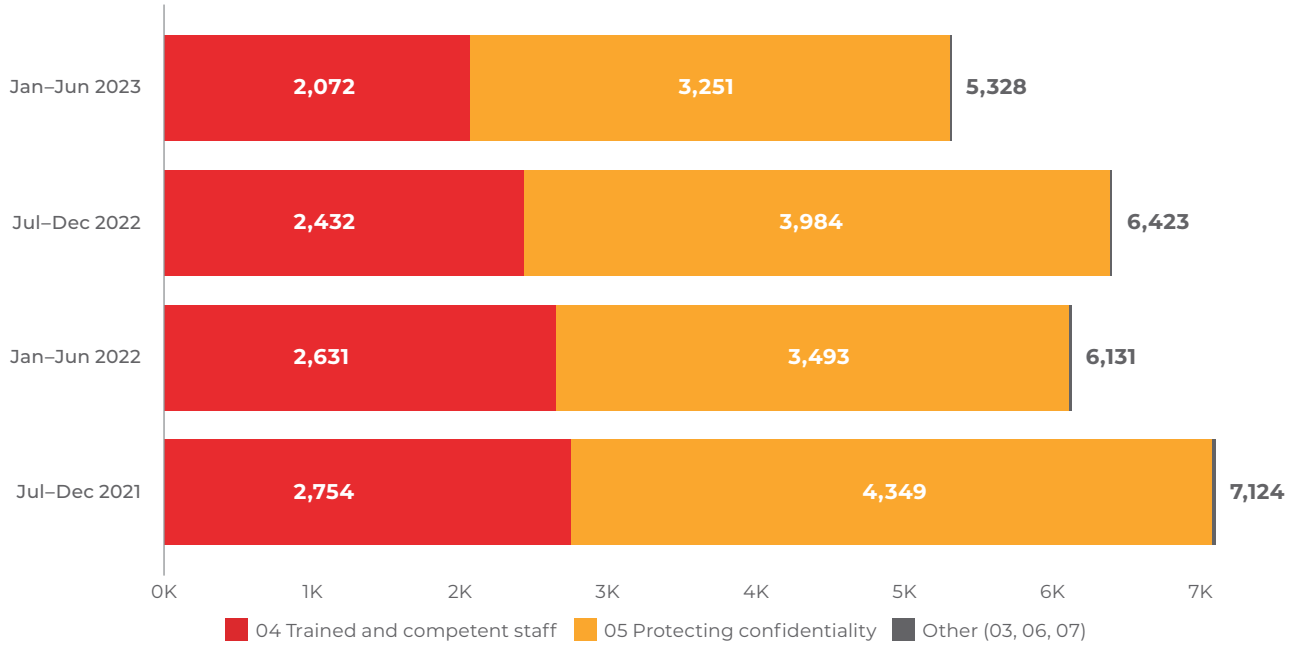


Chart 9: Breaches of Part 3 by Chapter

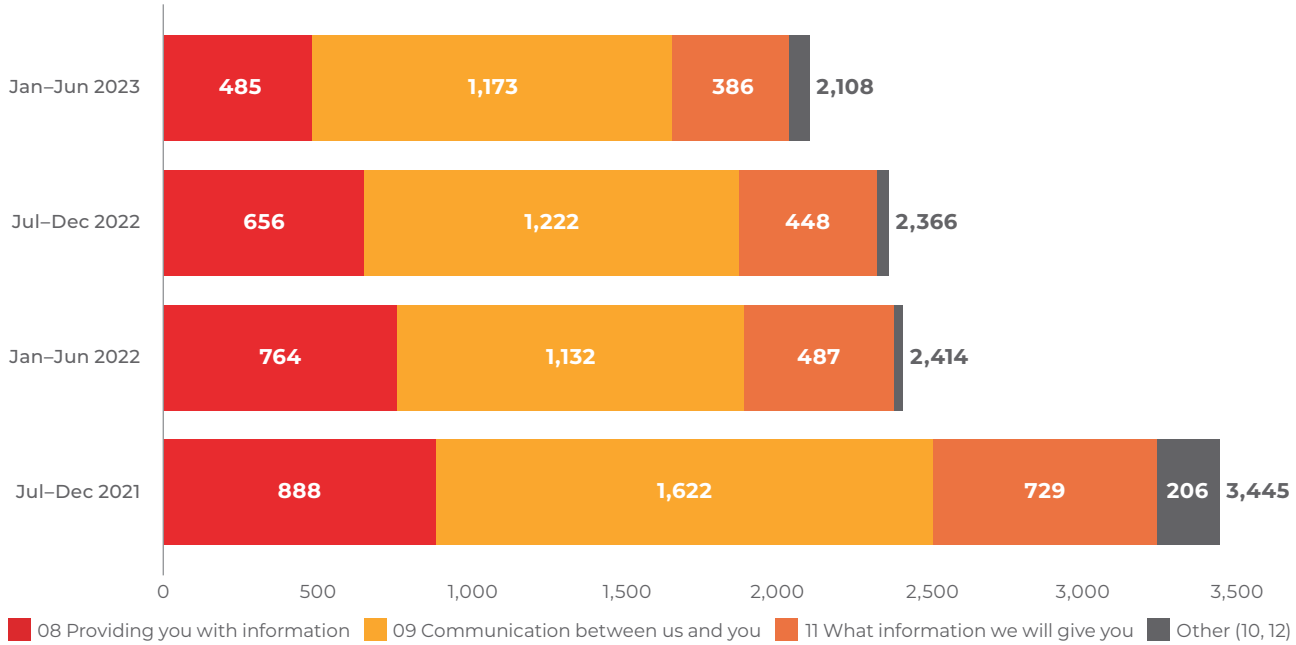


Chart 10: Breaches of Part 4 by Chapter

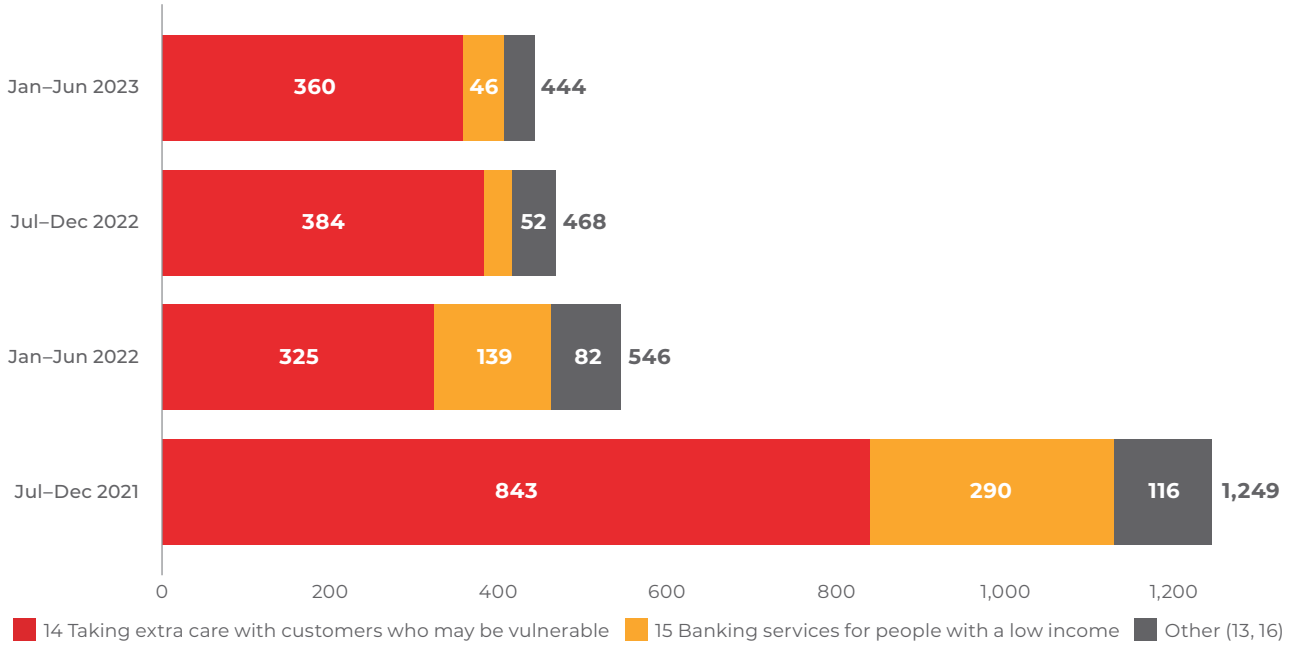


Chart 11: Breaches of Part 5 by Chapter

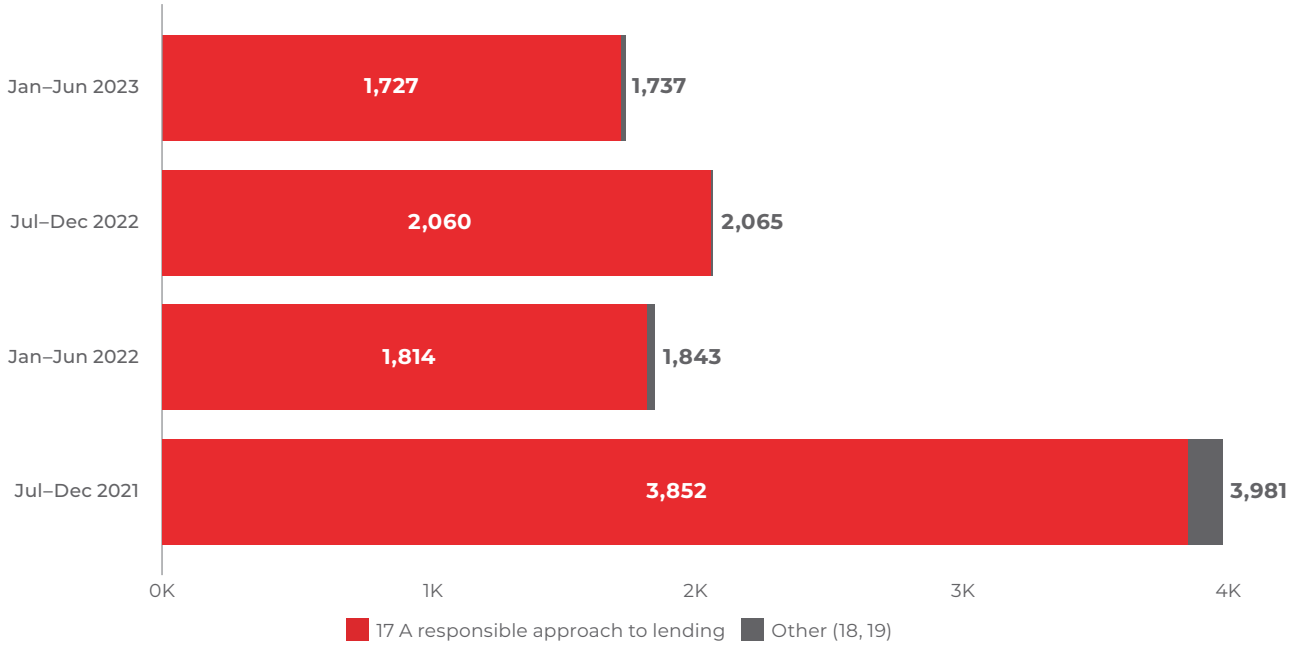


Chart 12: Breaches of Part 6 by Chapter

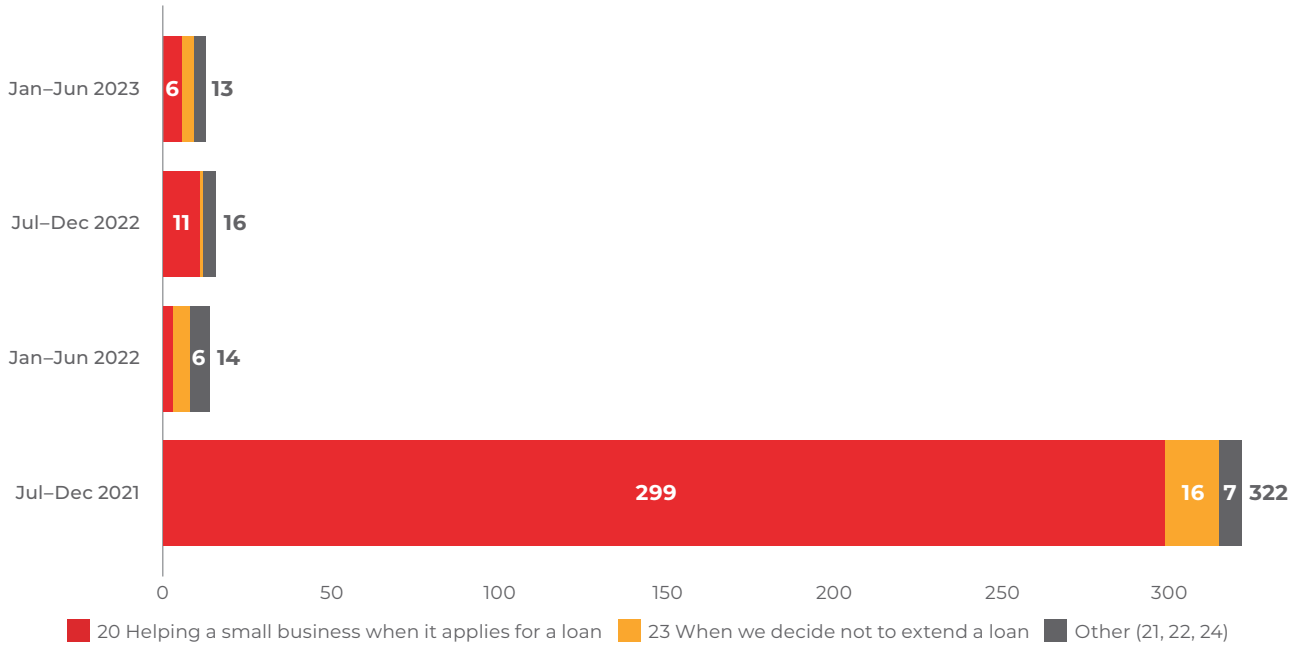


Chart 13: Breaches of Part 7 by Chapter

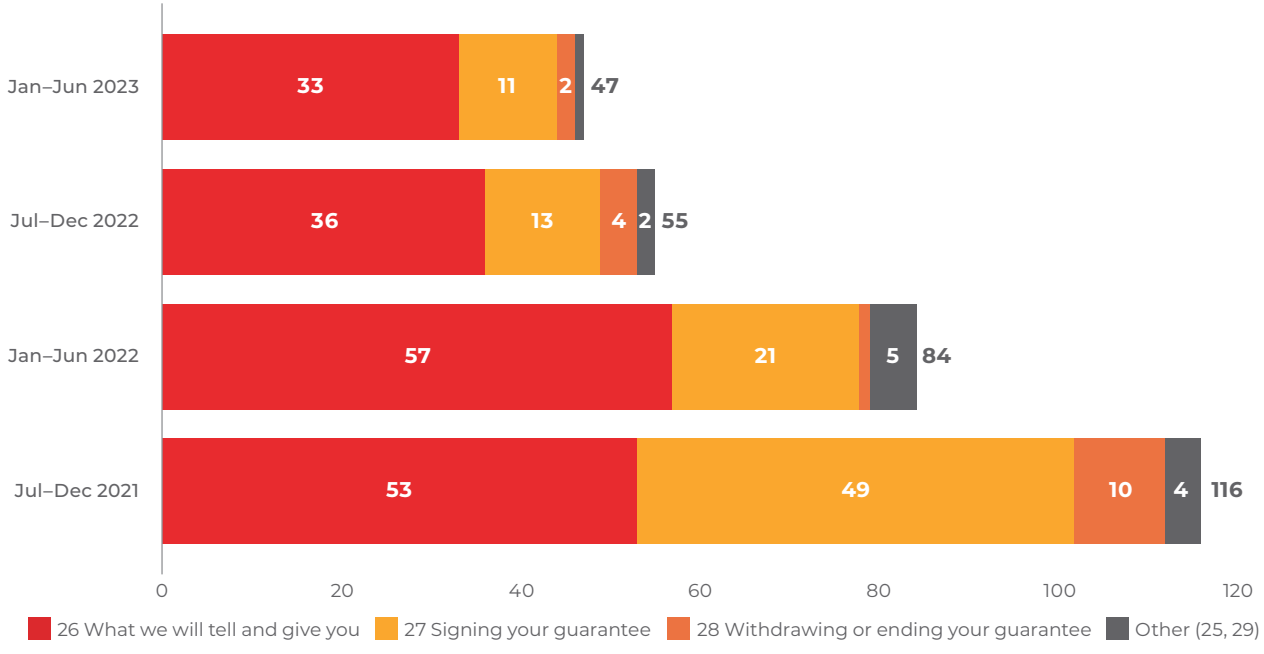
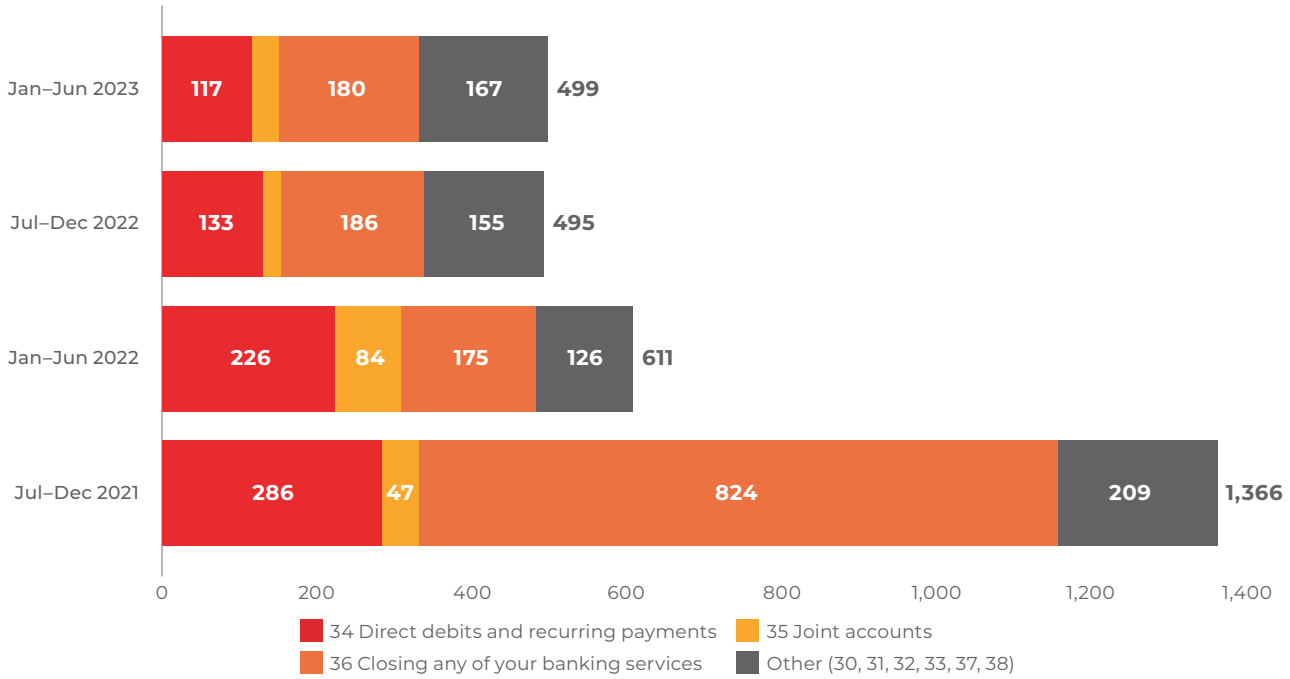


Chart 14: Breaches of Part 8 by Chapter



Note: This Chart was updated to correct the labels for Ch 35 and 36 on 15 December 2023.

Chart 15: Breaches of Part 9 by Chapter

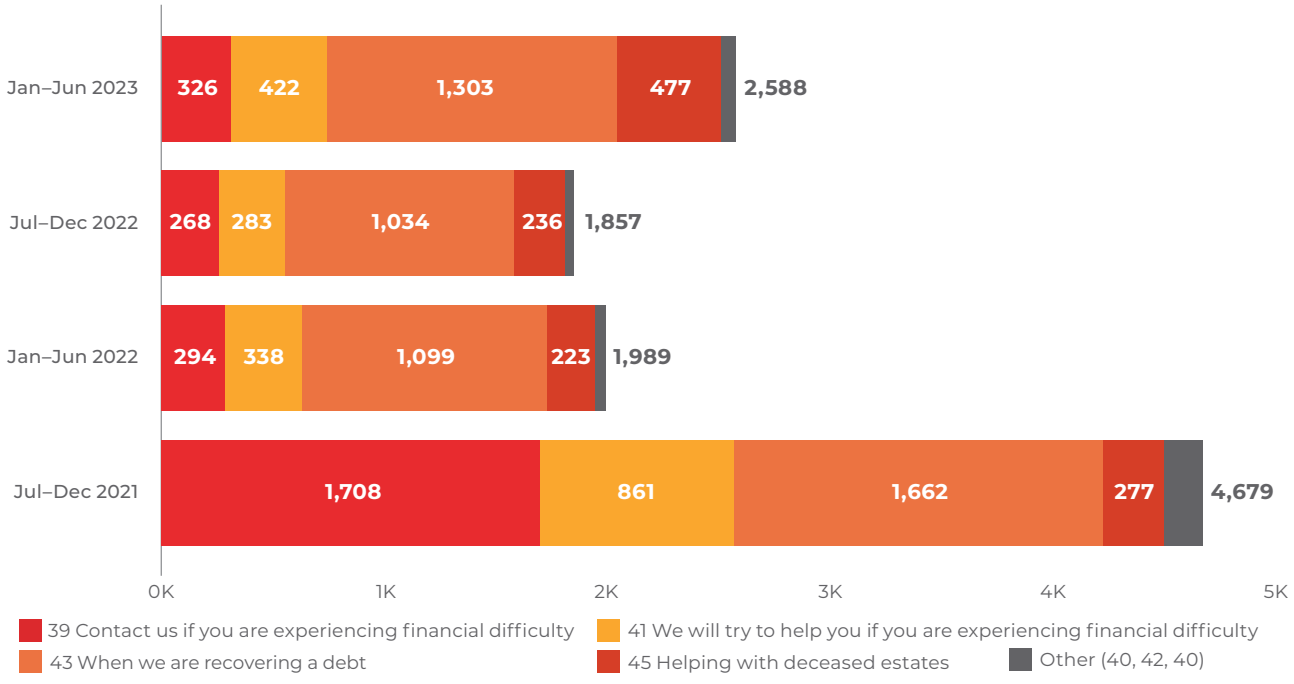
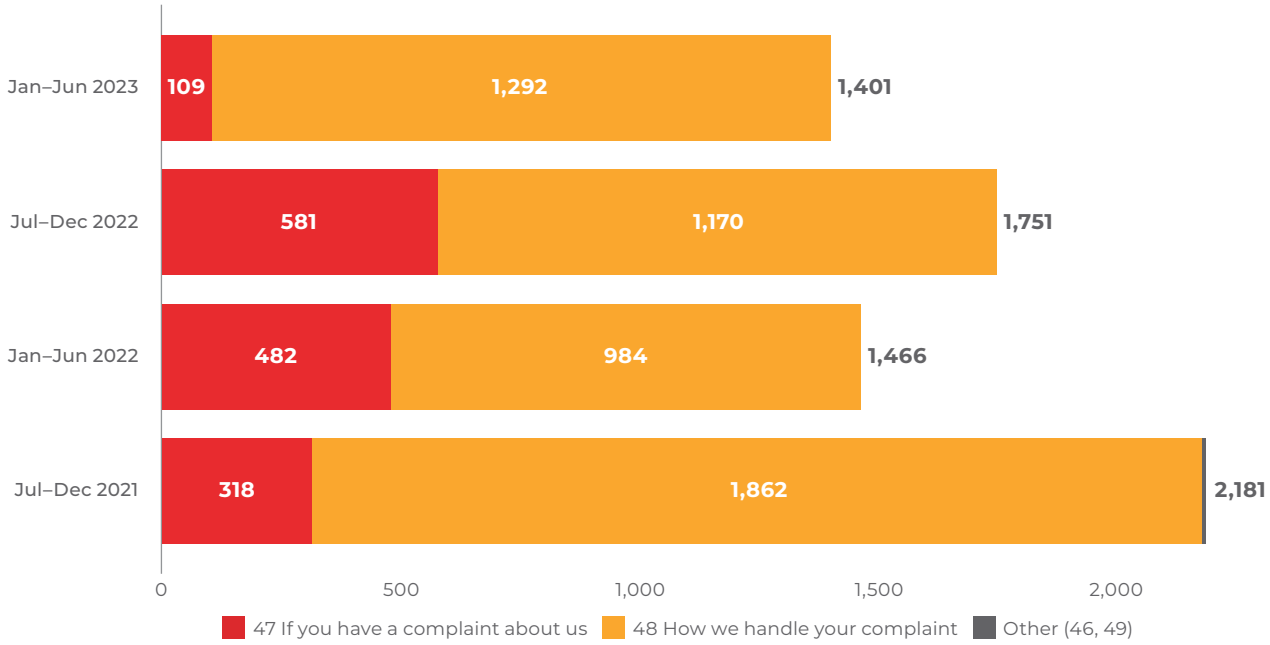


Chart 16: Breaches of Part 10 by Chapter



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.