Compliance with the Banking Code of Practice

January – June 2022

BCCC
Banking Code
Compliance Committee

Contents

Chair's message

I am pleased to present our latest report on compliance with the Banking Code of Practice (the Code). This report covers breaches reported between January and June 2022.

Significant decrease in self-reported breaches

The good news from the reporting period is the unprecedented 38% decrease in self-reported breaches.

The decrease is a great result and indicates the work to improve systems and processes is producing the desired effects.

We heard from banks that there were several factors at play for this decrease. These included:

- promoting awareness of Code obligations among staff through focused training
- focusing on the root causes of breaches and resolving underlying issues
- identifying and categorising breaches more accurately
- improving systems and processes following regulatory change.

We note the 20% reduction in breaches of Chapter 5: Protecting confidentiality. This has been consistently one of the most common sources of breaches, and the reduction demonstrates an effort to get on top of the underlying issues.

While the reduction is positive, this remains the Chapter with the highest number of breaches. In a time of increasing concerns about privacy and personal data, this is something that banks need to take seriously.

Quality of submissions

While the downward trend in breaches is positive, we continued to see issues with the quality of the submissions we received.

Banks must report breaches against the right Code obligation and use better descriptions of breaches.

Too often we receive notifications with descriptions that are too broad and overuse internal jargon without further explanation.

On top of this, banks need to ensure that their submissions are complete.

We saw errors in the required sample data which indicate a concerning lack of care in preparing submissions. Banks need to provide data that is free of errors and meets the criteria in the BCCC's Guidance Note 1 - Breach Identification and Reporting (Guidance Note).

Improving compliance reporting

In implementing the 10 recommendations from the BCCC review that are within our remit, we continue to refine our Compliance Statement and the way we collect data.

Working closely with the Australian Banking Association (ABA) and banks, we plan to complete this work in 2024 and will publish updates on our progress as we go.

Ian Govey AM
Independent Chair
Banking Code Compliance Committee

Introduction

One of the main ways we monitor compliance with the Code is through the Compliance Statement.

Banks must provide data about their breaches twice a year in the Compliance Statement, each time reporting on the preceding six-month period.

This report summarises the data from the reporting period of January – June 2022.

In the Compliance Statement, a bank must report the total number of breaches it 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 banks to report the details of each breach by describing the incident, event or action and then listing one or more Code obligations that were breached.

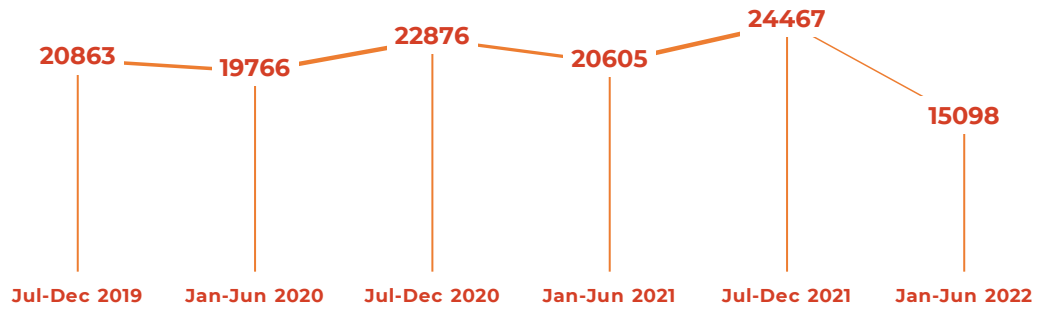
The data in this report has been de-identified. Each of the largest four banks are referred to as 'major bank' and the other banks are referred to as 'bank'.

More information about us and the Compliance Statement can be found in the Appendix.

Overview of breaches

In this reporting period, we observed a 38% decrease in self-reported breaches. This follows the 19% increase reported in the preceding reporting period.

Chart 1: Total breaches over most recent six reporting periods



For the first time we observed a reduction in all parts of the Code.

All 4 major banks reported a decrease in breaches in this reporting period, and only 4 out of 18 subscriber banks reported an increase (compared to 10 out of 18 banks in the last period).

The explanations we received for the decrease included:

- enhanced focus on staff training to improve awareness of Code obligations
- efforts to increase staff capabilities
- adjustments to reporting processes that better identify and categorise breaches
- more carefully and accurately categorising breaches
- improvements to systems and processes in response to regulatory changes.

Code breaches by Part

The Code is made up of 10 Parts. Each Part comprises Chapters which detail obligations about service standards for specific aspects banking.

While noting that they have the most customers, the major banks accounted for 87% (13,093) of the breaches reported in this period.

Table 1: Breaches by Part of the Code

Code Part	Breaches	Change from previous period
Part 2 Your banking relationship	6,131	↓ 14%
Part 3 Opening an account and using our banking services	2,414	↓ 30%
Part 9 When things go wrong	1,989	↓ 57%
Part 5 When you apply for a loan	1,843	↓ 54%
Part 10 Resolving your complaint	1,466	↓ 33%
Part 8 Managing your account	611	↓ 55%
Part 4 Inclusive and accessible banking	546	↓ 56%
Part 7 Guaranteeing a loan	84	↓ 28%
Part 6 Lending to small business	14	↓ 96%
Part 1 How the Code works	0	↓100%
Total	**15,098**	**↓ 38%**

Code breaches by Chapters

For six consecutive reporting periods, we have seen the most breaches of Chapters 5, 4 and 17.

Table 2: Top 5 Code Chapters with the most breaches

Code Chapter	**Breaches**	**Change from previous period**
05 Protecting confidentiality	3,493	↓ 20%
04 Trained and competent staff	2,631	↓ 4%
17 A responsible approach to lending	1,814	↓ 53%
09 Communication between us and you	1,132	↓ 30%
43 When we are recovering a debt	1,099	↓ 34%

Table 3: Notable increases in breaches by Code Chapter

Code Chapter	Breaches	Change from previous period
35 Joint accounts	84	↑ 79%
33 Managing a credit card or debit card	34	↑ 70%
47 If you have a complaint about us	482	↑ 52%
32 Cost of transaction service fees	18	↑ 50%
16 Basic accounts or low or no fee accounts	59	↑ 20%

Table 4: Notable decreases in breaches by Code Chapter

Code Chapter	Breaches	Change from previous period
39 Contact us if you are experiencing financial difficulty	294	↓ 83%
36 Closing any of your banking services	175	↓ 79%
17 A responsible approach to lending	1,814	↓ 53%
48 How we handle your complaint	984	↓ 47%
05 Protecting confidentiality	3,493	↓ 20%

Statistics used in this report

Banks reported a total of 15,098 breaches for this reporting period.

Of the total, they provided further details for a sample of 7,483 breaches that came from 3,165 incidents. This is referred to as the 'breach sample'.

The details banks provided for the breach sample included information about the nature, cause, financial impact[1], customers affected, and correction of the breaches.

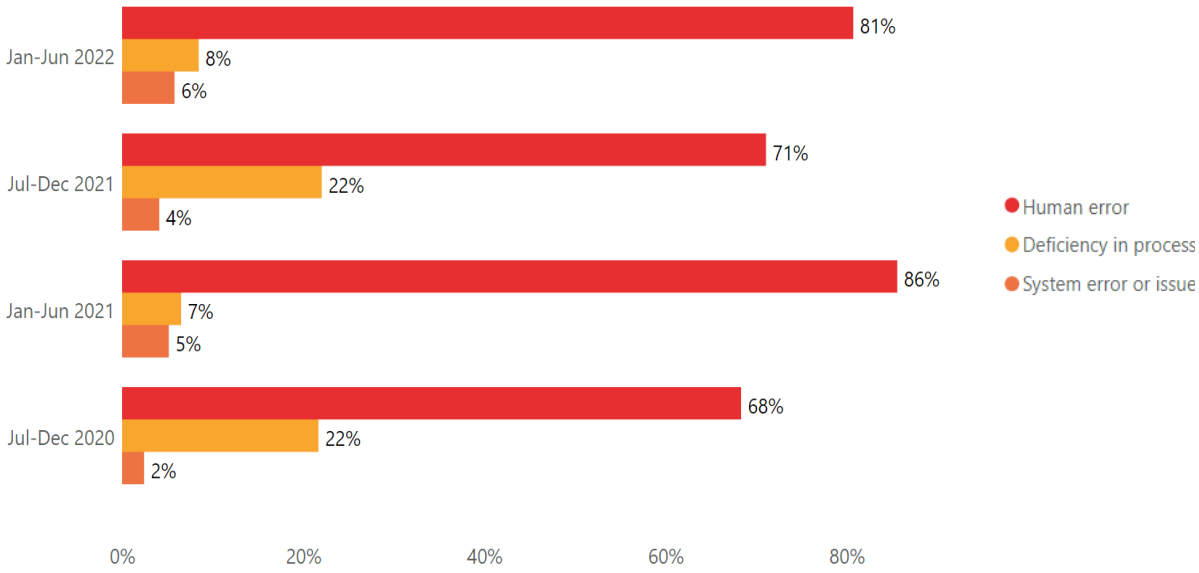
[1] Where this report refers to 'financial impact', this means either actual or estimated financial impact on the customer/s or the bank at the time of reporting.

Change in approach this period

In this report, information from the sample data has percentages based on breaches rather than incidents. (In previous reports, these percentages were based on incidents). This change better reflects the true scale and impact of breaches.

For any reference to figures from previous reporting periods in this report, we have taken the same approach to enable accurate comparisons.

Chart 2: Top 3 causes of breaches

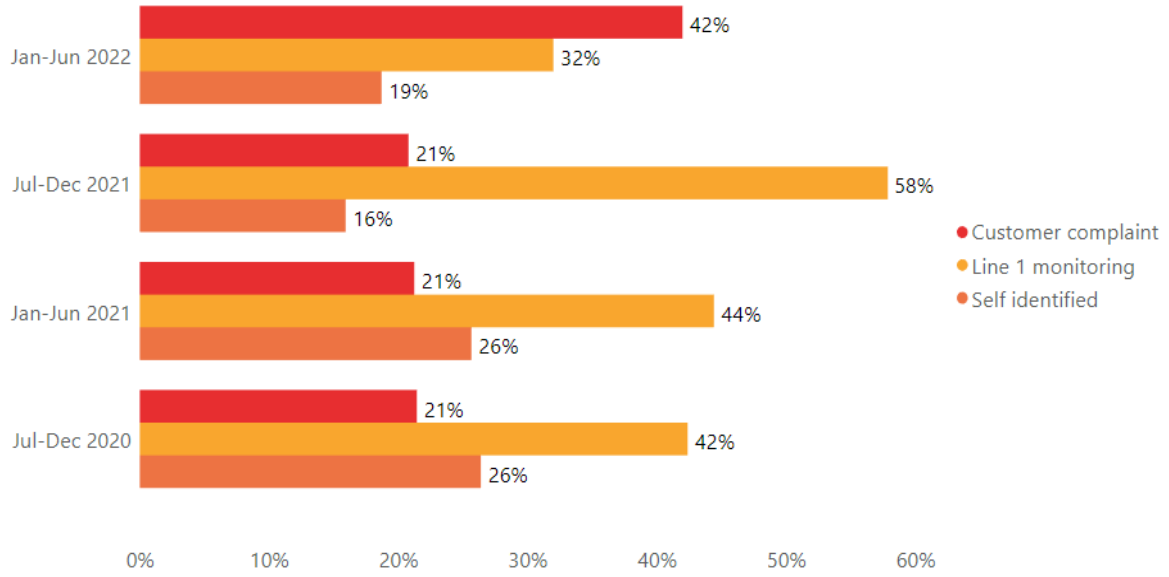


Human error continues to be the most common cause of breaches. Of the 7,483 sample breaches, 6,041 (81%) were attributed to human error.

In our report Building Organisational Capability, we identified that banks too often identify human error as the cause of breaches without establishing, recording or acting on the root cause of the problem.

For breaches attributed to human error, often staff conduct was influenced or constrained by systems, processes, technology, training or organisational culture. A lack of consideration for the root cause may inhibit long-term solutions.

Chart 3: Top 3 sources for identifying breaches



The proportion of breaches identified through customer complaints doubled in this reporting period.

This may be the result of regulatory change with Regulatory Guide 271: Internal Dispute Resolution (RG 271) from Australian Securities and Investments Commission (ASIC) coming into effect.

This broadened the definition of a complaint in internal and external dispute resolution, leading to banks revising their approaches to identifying and recording complaints.

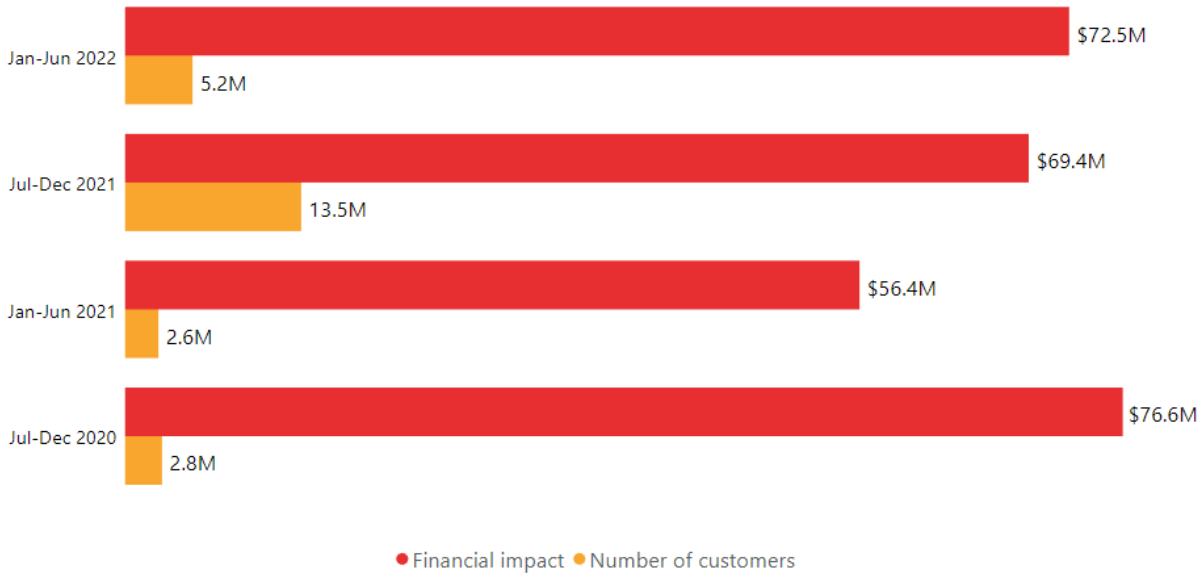
This is the first reporting period in which RG271 has been fully operational.

It offers banks an excellent opportunity to review complaints data and detect Code breaches that may not have otherwise been captured.

It will also encourage banks to improve processes and systems to prevent issues from recurring.

We expect breach identification by customer complaints to reduce over time as the measures to comply with RG271 mature.

Chart 4: Impact of breaches



The 5.2 million affected customers in the sample from this reporting period is a significant drop from the 13.5 million in the previous reporting period. However, the financial impact of $72.5 million is an increase on the $69.3 million of the last period.

This points to breaches of significant financial impact that affected fewer customers.

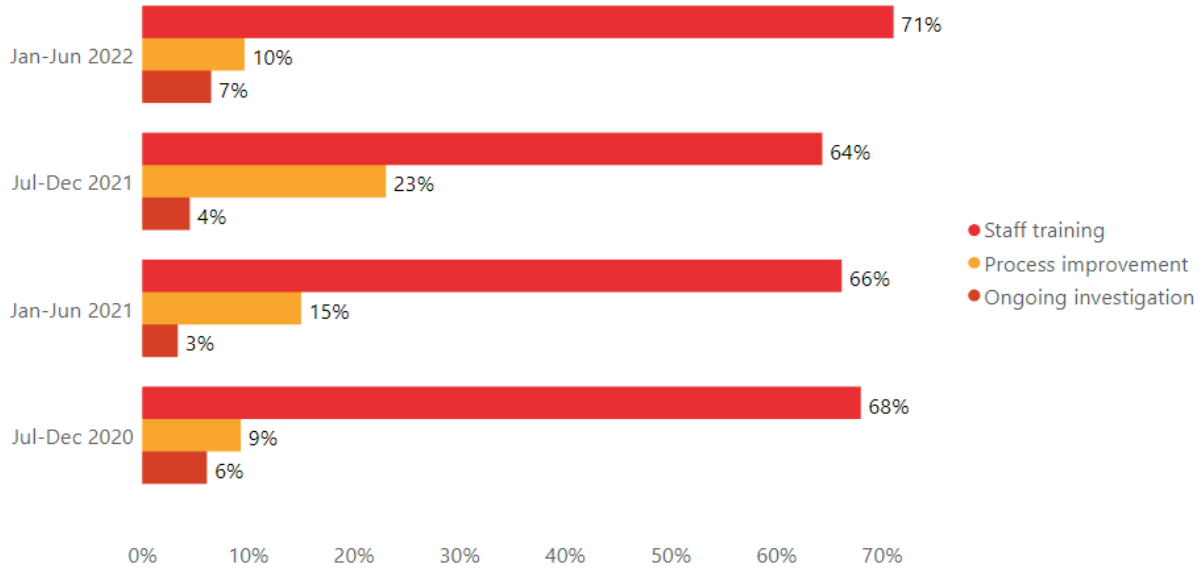
Nevertheless one breach from a major bank had a financial impact of $12.3 million and affected over 2,500 customers.

And another single breach, which affected 270,000 customers, had a financial impact of over $5 million.

The top 3 breaches by financial impact in this period accounted for $23.3 million, up from $17.8 million in the last reporting period.

The top 3 breaches by affected customers accounted for 2.6 million people, down from 9.5 million.

Chart 5: Top 3 corrective actions taken in response to breaches



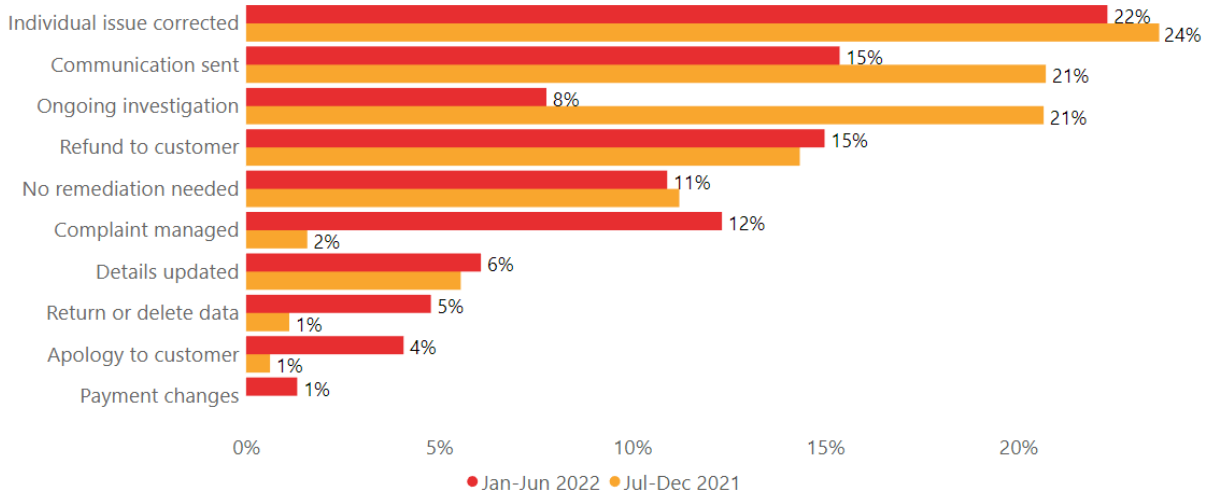
Staff training continued to be the most common corrective action in response to breaches. This matches the prevalence of human error as the cause of reported breaches.

When viewed with the drop in process improvement as corrective action, this indicates that banks view these as isolated lapses in staff performance, rather than deeper issues that may be fixed with improvements to systems and processes.

While it is important to address staff performance by investing in training and improvements, banks should review breaches to see if system or process issues are also involved.

It may be that improvements to systems and processes as corrective actions can lead to a reduction in human error being cited as the cause of most breaches.

Chart 6: Remediation of breaches



Correcting the individual issue was the most common remediation. While a refund was sometimes an option, the data indicates non-monetary remediation, such as an apology, correction or explanation, was more common.

This reporting period saw fewer reported as 'ongoing investigation' compared to the previous reporting period – a trend we hope will continue.

Compliance with the Banking Code

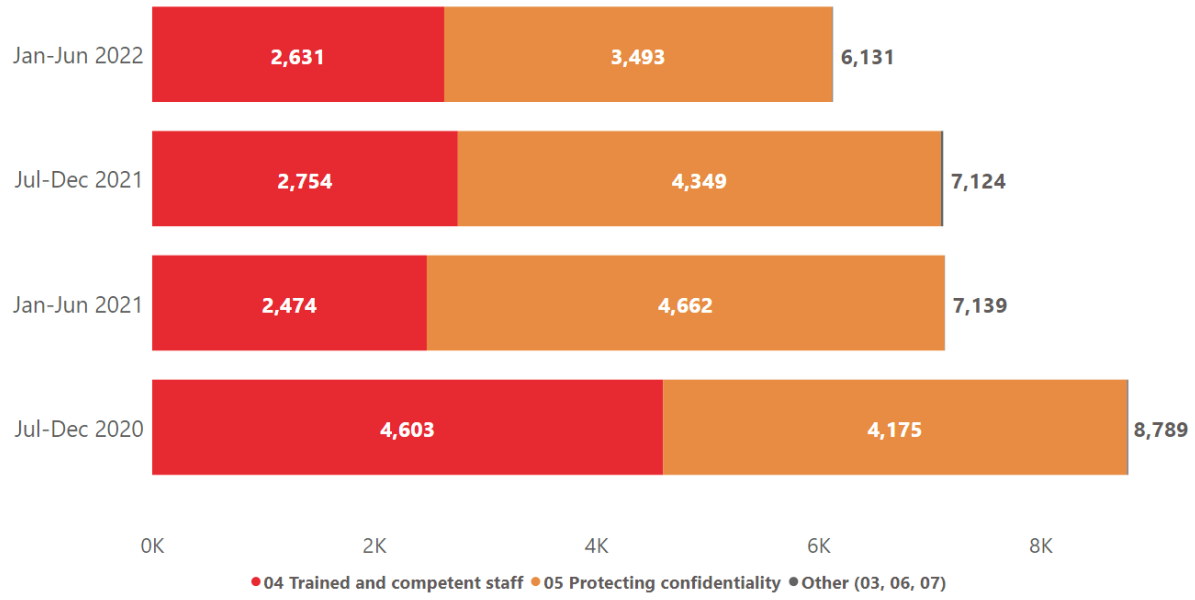
Part 2 Your Banking Relationship

Part 2 of the Code requires banks to comply with the Code and relevant laws, ensure their staff and representatives are trained and competent, protect the confidentiality of their customers and comply with the ABA protocol when closing a branch.

Part 2 has consistently had the highest number of breaches.

In this reporting period, Part 2 breaches accounted for 41% of all breaches. While this is significant, there was a 14% decrease in breaches of Part 2 (6,131) compared to the previous reporting period (7,124).

Chart 7: Breaches of Part 2 by Chapter



Almost all breaches of Part 2 concern Chapter 4 – Trained and competent staff and Chapter 5 – Protecting confidentiality.

Chapter 4 – Trained and competent staff

Chapter 4 includes two important obligations:

- to have trained and competent staff
- that staff will engage with customers in a fair, reasonable and ethical manner.

These obligations underpin compliance with most other Code obligations.

Despite the slight decrease overall of 4% in the number of Chapter 4 breaches (2,631) compared to the last reporting period (2,754), 11 of the 18 banks reported an increase, including 3 major banks.

Of the increase reported by these 11 banks, the major banks accounted for 85%.

Table 5: Examples of Chapter 4 breaches and the customers affected

Breaches	Customers affected
Incorrect reporting or suppressing repayment history information	382,488
Incorrect interest rate discounts applied to home loan accounts	33,160
Incorrect charging of discharge fees	22,007
Incorrect charging of ATM fees	16,951
Marketing materials sent to a customer who had opted out of marketing communications	61,315
Incorrect contact number displayed on the bank's website	66,028*

* Based on the number of customer visits to the pages with the incorrect information.

The sample data for Part 2, Chapter 4 comprised 1,108 incidents, which involved 1,699 breaches. This represents 65% of Chapter 4 breaches.

The sample data showed breaches of Chapter 4 contributed to a financial impact of $51.5 million and affected 1.1 million customers.

Our analysis also revealed a persistent issue of banks incorrectly reporting the relevant breaches of the Code.

Chapter 4 obligations relate to staff conduct, but banks reported several breaches caused by system errors. Based on the descriptions banks provided, it is unclear how the incidents resulted in a breach of Chapter 4.

For example, the following incidents were reported as breaches of Chapter 4 (as well as other Chapters):

- A system issue with internet banking resulted in a payment being made three times.
- A customer's offset account was delinked due to a system issue.

- A system issue resulted in the incorrect calculation of arrears for two accounts.

We urge banks to review their reporting and identify breaches of the Code accurately. Errors in reporting not only reflect poorly on a bank's capacity to account for its performance, but they also offer little for a bank to learn from and improve.

Chapter 5 - Protecting Confidentiality

Chapter 5 is consistently the Chapter with the highest number of breaches. It sets out obligations regarding privacy and confidentiality.

Although it remained the Chapter with the most breaches in this reporting period (3,493), it did see a 20% decrease.

However, the results were mixed across the banks. While 11 reported a decrease (including 3 major banks), 5 reported an increase.

While a reduction in breaches is positive, the number remains high. In a time of heightened concerns about privacy and personal data, this is something that banks must take seriously.

The sample data for Part 2, Chapter 5 comprised 767 incidents, which involved 1,190 breaches. This represents 34% of the total Chapter 5 breaches.

The sample data showed breaches of Chapter 5 contributed to a financial impact of $2.0 million and affected 124,917 customers.

Table 6: Examples of Chapter 5 breaches that affected large numbers of customers

Breaches	Customers affected
Uploading information that identified a customer to a third-party website	52,200
Staff member sending an email containing customer data to their personal email account	33,000
Sharing a data file containing customer information with an external supplier	9,105
Sending customer account numbers to an unauthorised external party in error	5,763
Sending a replacement credit card to an old address instead of the updated address	3,109

Breaches of this nature are avoidable, and banks must improve their systems and processes to minimise them.

We encourage efforts to train staff on better compliance with Chapter 5 obligations, but it is important that banks explore how system and process improvements can help.

Chart 8: Cause of breaches of Part 2

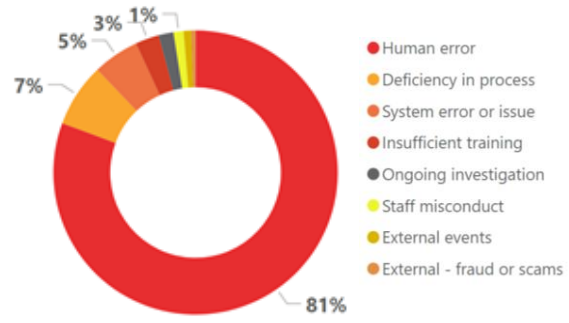


Chart 9: Identification of breaches of Part 2

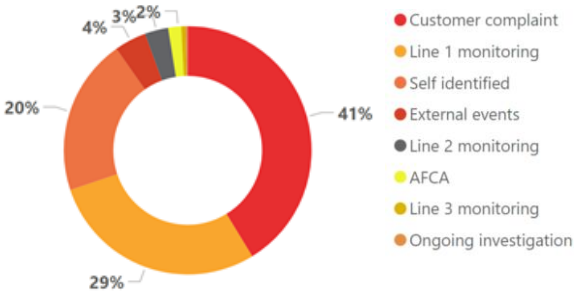


Chart 10: Remediation of breaches of Part 2

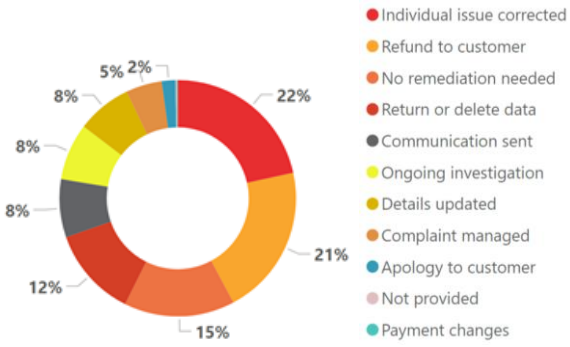
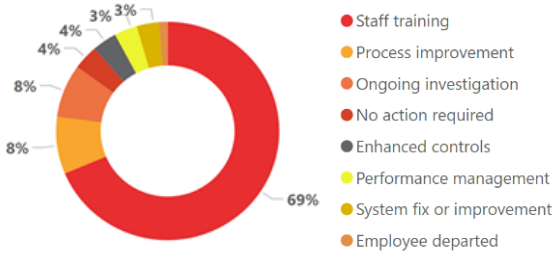


Chart 11: Corrective action taken in response to breaches of Part 2



Part 3 Opening an account and using our banking services

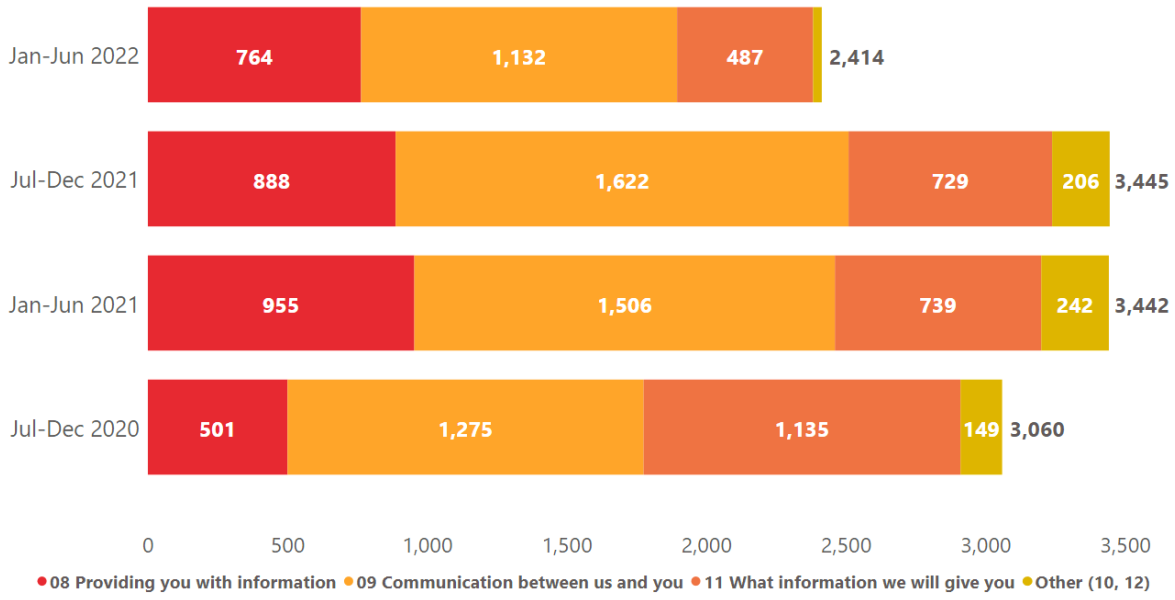
Part 3 specifies how banks must communicate with customers and that the information they provide needs to be clear. It also contains requirements about the contents of terms and conditions.

Breaches of Part 3 came down by 30% in this reporting period.

Although there was a decrease in the number of breaches, this was attributed in part to one bank refining its reporting of Part 3 breaches, leading to classification in other Parts.

Another bank attributed its significant decrease to the reduced number of breaches of Chapter 48 (How we handle your complaints), which often related to untimely communication to customers about their complaints.

Chart 12: Breaches of Part 3 by Chapter



Three major banks accounted for 83% (1,991) of the total Part 3 breaches. All other banks except one reported fewer than 100 breaches.

Chapter 9

An important aspect of Part 3 of the Code is Chapter 9, which has obligations for communicating with customers.

This Chapter saw the highest number of breaches from Part 3, with a total of 1,132. Although the number remains high, and these breaches remain a concern, it is a 30% drop on the previous period.

One major bank previously reported failures to issue a Financial Services Guide as a breach of Chapter 9, but it now reports these breaches under Chapter 8. This contributed to the decrease of Chapter 9 breaches.

The sample data revealed examples of breaches of the obligations in Chapter 9 regarding communication with customers:

- One major bank incorrectly issued notification to 123 customers that their financial hardship arrangement had been breached. This was caused by a system error that failed to apply the customers' payments to their accounts.
- One major bank did not provide 10 customers with clear information on the impacts of entering a financial hardship arrangement with the bank. This resulted in $19,000 in financial impact.
- One major bank mistakenly informed 246,000 customers that their minimum home loan repayments would be decreasing in January 2023 instead of January 2022.
- One bank sent 35,000 customers correspondence to an address not nominated by them.
- One major bank provided 1.3 million customers with outdated information about fees and an incorrect link to the bank's website.

Breach sample

The sample data for Part 3 comprised 706 incidents, which included 1,189 breaches. This represents 49% of the total Part 3 breaches.

Of the 706 incidents, 405 contained breaches of Part 3 alone (820 breaches). The remaining 301 incidents included 369 breaches of Part 3 and other Parts of the Code.

These incidents affected 3.6 million customers and had a financial impact of $25.9 million.

The sample data showed:

- breaches reported by one major bank accounted for more than 80% of the financial impact ($21.4 million) and nearly half of the affected customers (1.7 million)
- three major banks accounted for 97% of the financial impact ($25.3 million), affecting 2.5 million customers.

The breaches of Part 3 with the largest financial impact:

- One major bank charged an unarranged lending rate or overdue interest on matured business lending facilities. This affected 2,500 customers and resulted in over $12.2 million in financial impact. The bank corrected the error and improved its process and enhanced its monitoring and controls.
- One major bank's online banking platform displayed the incorrect amount of available funds for 270,000 customers. This was caused by a system failure and was soon fixed, but it resulted in financial impact of $5.0 million.
- Another major bank incorrectly amended its terms and conditions which resulted in fees being charged to small business customers. This was

caused by human error and the bank provided training to staff in response, but it resulted in financial impact of $1.5 million.

Human error was the main cause of breaches of Part 3 (70%). The most common corrective action was staff training and feedback.

Chart 13: Cause of breaches of Part 3

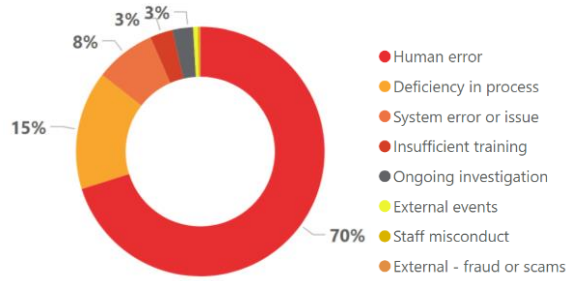


Chart 14: Identification of breaches of Part 3

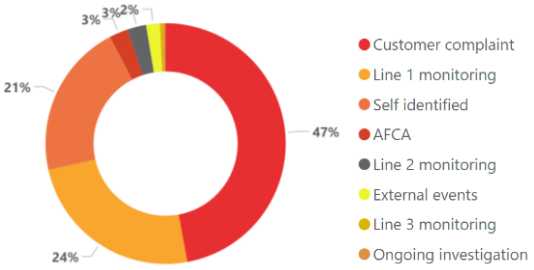


Chart 15: Remediation of breaches of Part 3

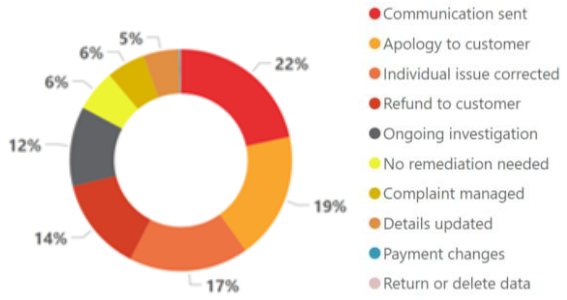
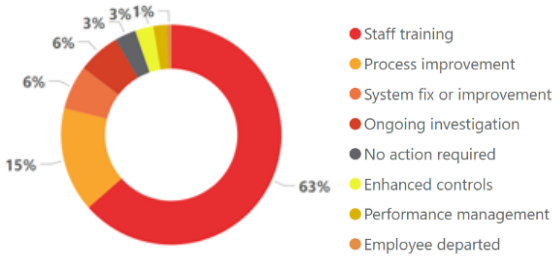


Chart 16: Corrective action taken in response to breaches of Part 3



Part 4 Inclusive and accessible banking

Part 4 requires banks to provide inclusive and accessible banking services.

This includes taking care to consider services for people on low incomes and taking extra care with customers who may be experiencing vulnerability.

SPOTLIGHT – Inclusivity and vulnerability

Charging fees on basic, low-fee or no-fee accounts

The obligation
In Part 4 of the Code, Chapters 15 and 16 relate to banking services for people with a low income and providing basic accounts or low or no fee accounts.

Such initiatives promote financial and social inclusion by helping individuals to greater financial well-being.

What we saw
One major bank charged 222 customers account fees that were not applicable due to special features on the account. This was caused by a system error and resulted in $8,700 of financial impact. The bank refunded the customers and fixed the error in the system.

What we expect
Although the financial impact appears to be relatively low, the risk of consumer harm is higher because the customers who hold accounts with these special features often have low incomes.

It is unclear how long it took the bank to remediate the affected customers. But doing so quickly is crucial to minimising potential harm. We encourage banks to expedite the rectification of such breaches.

Failing to take extra care when dealing with customers undergoing separation or experiencing family or domestic violence

The obligation
Chapter 14 includes the obligation to take extra care with customers who are experiencing vulnerability, including family or domestic violence.

Extra care includes ensuring staff are equipped to manage these circumstances, and it means treating customers with sensitivity, respect and compassion.

Banks must take seriously the confidentiality of information from customers experiencing family or domestic violence because of the risks to their personal safety and wellbeing.

What we saw

- One major bank disclosed the mailing address of a customer experiencing domestic violence to their former partner. This occurred when the bank updated the customer's mailing address on the account,

including a joint account held with the former partner. The breach was identified through a customer complaint.

- Another major bank mailed a post settlement letter with a customer's updated address to the customer and the customer's former partner, against whom they had a court order. The breach was identified through a customer complaint.

- One bank provided a customer's former partner with a loan agreement and security details related to the customer. The breach was identified through a customer complaint.

- One major bank failed to block all joint accounts when it was advised of the customer's separation from their partner. This resulted in the customer's former partner transferring a significant amount of money out of the joint accounts. The breach was identified through a customer complaint.

- Another major bank failed to delink a customer's account from their former partner which resulted in an unauthorised withdrawal. The breach was identified by bank staff.

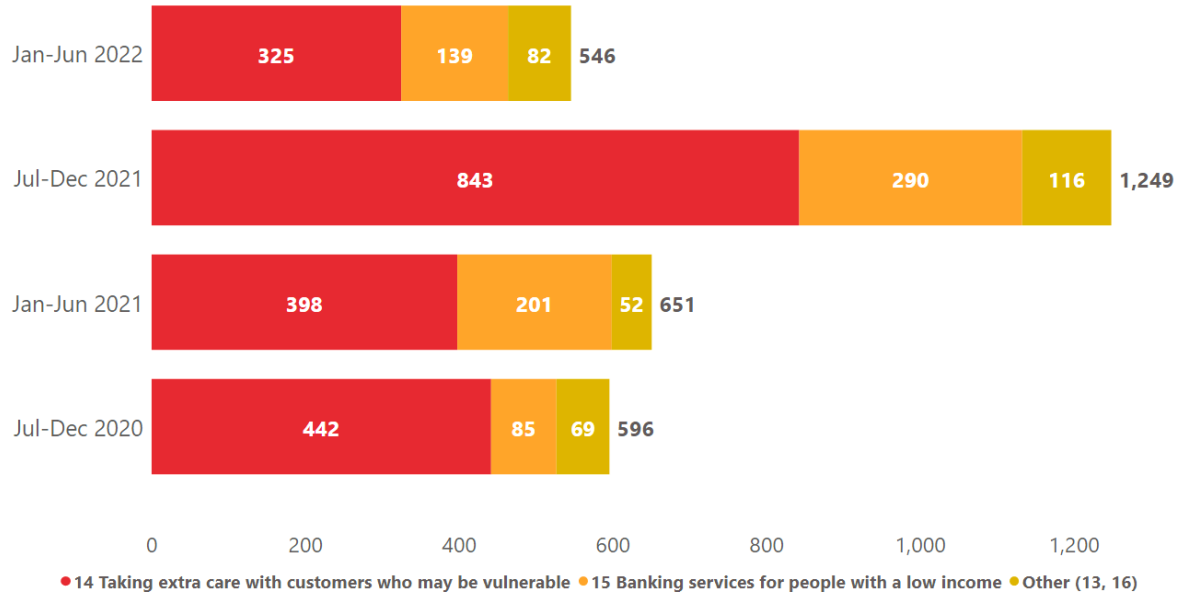
What we expect
These incidents highlight the importance of the obligations to protect customers experiencing vulnerability and the serious potential consequences of breaches.

The incidents were all caused by human error and all, except one, were rectified with staff training. However, it is important that banks realise that many incidents are complex and meeting obligations requires a multi-faceted approach.

We expect banks to have controls in place beyond training in situations where staff deal with customers experiencing vulnerability. The Industry Guideline on preventing and responding to family and domestic violence provides guidance on how banks can meet their obligations.

For the first time since 2019, banks reported a decrease in breaches of Part 4. It is a significant drop of 56% on the previous reporting period.

Chart 17: Breaches of Part 4 by Chapter



Banks reported improved processes, technology and greater awareness from staff about obligations as the main contributing factors to the decrease. For example:

- Establishing a system that supports leaders managing key activities such as ongoing observations, coaching and risk.
- Requiring staff to complete mandatory observations set out in a customer care guide to ensure appropriate care is provided to vulnerable customers.
- Using an enhanced speech analytics tool to identify language commonly used by potentially vulnerable customers.

Within Part 4 of the Code, breaches of Chapter 14, which requires banks to take extra care with customers who may be experiencing vulnerability, remain the highest. But the 61% decrease in these breaches is a good result.

Examples of breaches of Chapter 14:

- Charging fees on no-fee accounts.
- Failing to take extra care when dealing with customers undergoing separation or experiencing domestic violence.

Despite the overall decrease, some banks observed more breaches of Chapter 14 in this reporting period.

According to the sample data provided, one bank attributed its increase to changes in its approach to classifying complaints separate to feedback. The other banks did not provide further information on the increases as they did not meet the threshold set out in the Guidance Note to provide this detail.

Bucking the trend of decreases in Part 4 was Chapter 16 and its requirements for basic, low-fee or no-fee accounts. Breaches of this Chapter have increased since 2019, with this reporting period seeing another 20% rise.

The type of breaches reported included failing to raise awareness of basic, low-fee or no-fee accounts and charging fees that should have been waived. As an example, one bank failed to provide information about an account designed for low-income earners and government benefit recipients to 121 eligible customers.

While the breaches are relatively low in numbers, the persistent upward trend raises concerns. In the current economic climate with increasing financial pressure on households, banks must improve in this area.

Our inquiry into inclusivity, accessibility and vulnerability strongly encouraged banks, at recommendation 16, to use data to identify customers eligible for a basic account and support them to product switch products. Banks should not rely solely on a customer disclosing a low income.

We will follow up on the progress banks have made in response to this inquiry in 2023.

Breach sample

The sample data for Part 4 comprised 117 incidents, including 154 breaches. This represents 28% of the total Part 4 breaches.

Of the 117 incidents, 47 contained breaches of Part 4 alone (61 breaches). The remaining 70 incidents included 93 breaches of Part 4 and other Parts of the Code.

These incidents affected 6,825 customers and had a financial impact of $893,850.

The financial impact and the number of customers affected by Part 4 breaches are significantly lower compared to the previous reporting period (47,743 customers and $2.4 million).

Chart 18: Cause of breaches of Part 4

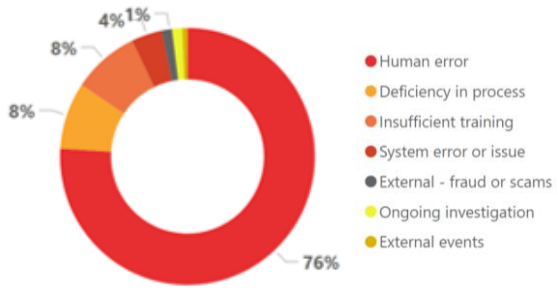


Chart 19: Identification of breaches of Part 4

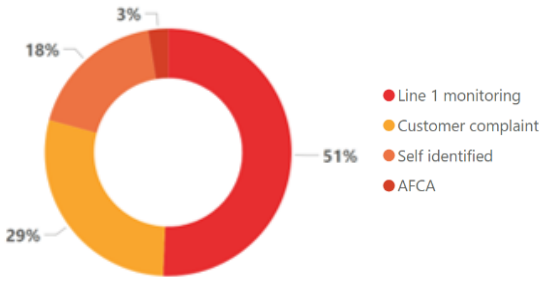


Chart 20: Remediation of breaches of Part 4

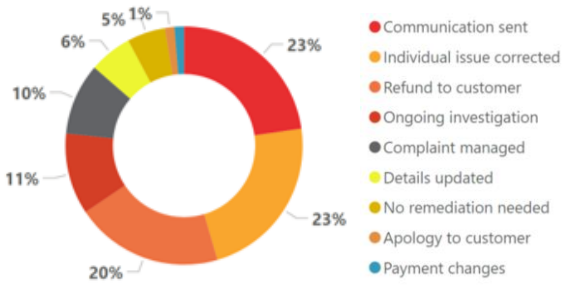
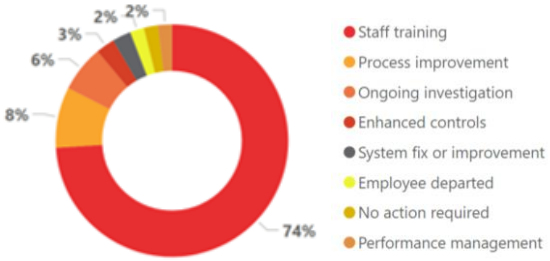


Chart 21: Corrective action taken in response to breaches of Part 4



Part 5 When you apply for a loan

Part 5 has obligations to ensure responsible lending, covered by Chapter 17. It also sets out requirements for selling consumer credit insurance (CCI) in Chapter 18 and lenders mortgage insurance (LMI) in Chapter 19.

SPOTLIGHT – Responsible lending

Exercising the care and skill of a diligent and prudent banker

The obligation
Chapter 17 requires banks to exercise the care and skill of a diligent and prudent banker when lending to individuals and small businesses.

The bank must not arrange a credit product that is unsuitable for a customer.

Banks must undertake a series of checks before approving credit to avoid customers accessing money that they cannot afford to pay back.

What we saw

- Between July 2019 to February 2020, one major bank reduced its credit checks so it could manage high volumes. The bank was concerned about meeting its obligations for responsible lending for the 650 home loans approved during this time.

  The bank's initial review found that 550 of the loans were unlikely to result in adverse customer impact, but 100 were. Of these, 25 were rated as high impact files, with 19 potentially being non-compliant with policy and 6 showing a servicing deficit. The bank will continue its review and initiate appropriate customer remediation.

- One bank's review of approved home loans found that it was unable to verify that the customers' income and liability had been calculated correctly. The breach was a result of staff not following the correct procedure for documenting information that would allow the bank to properly assess whether a customer could afford the credit.

- One bank reviewed home loan applications approved between 2011 and 2018 from customers who had since experienced financial hardship.

  The review found that the bank failed to properly assess whether the customers could afford the credit they were approved for by not verifying their income. This contributed to the subsequent hardship for the customers.

- One major bank reviewed loan files of customers who are now in financial hardship to see whether it had met its responsible lending obligations. The review found the bank failed to make reasonable inquiries of a customer's liabilities, such as Buy Now Pay Later limits and undisclosed debt debits, when assessing their ability to service the credit they were approved for.

- One major bank relied on an incorrect property valuation when it approved a loan to a customer. The bank relied on a valuation provided by a broker and failed to do its own checks.

  The valuation listed the residential site as an apartment which resulted in a valuation over the market value. The bank was unable to maintain the unconditional loan approval and the customer had to forfeit the purchase.

What we expect
Banks reported that these incidents were all caused by human error and rectified with staff training. However, banks, where possible, should consider incorporating measures beyond staff training to ensure they meet the obligations.

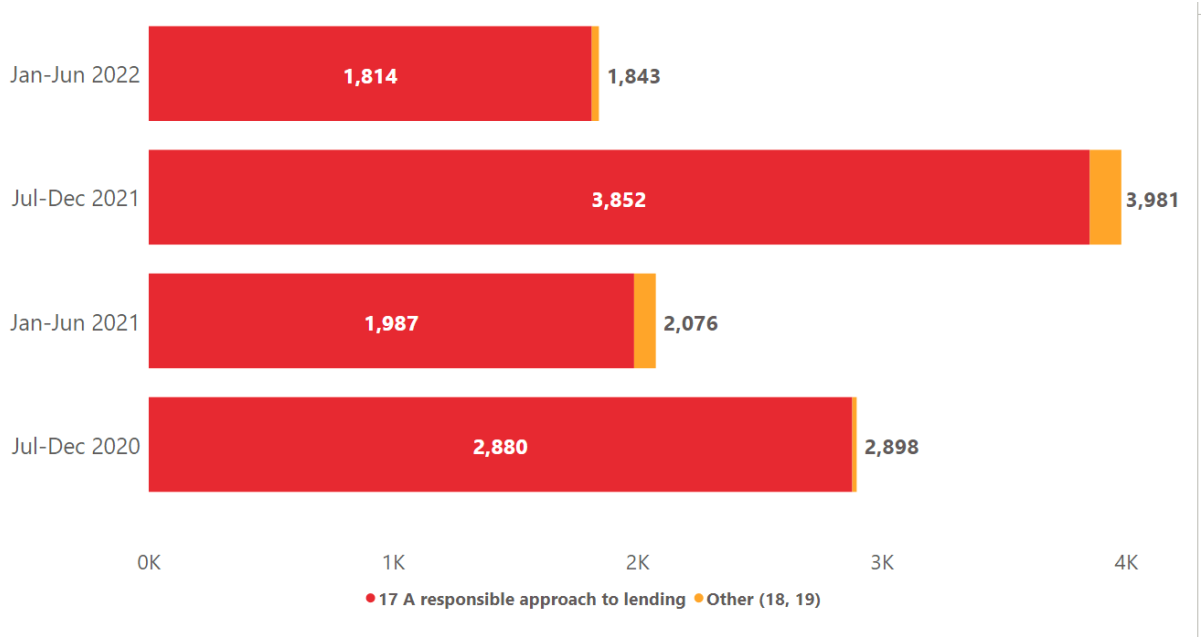
Such measures may include mandatory comprehensive checklists for assessing affordability before approving a loan and providing appropriate remediation.

In an environment of rising interest rates, inflation and challenges to household affordability, this is especially important.

Banks reported a 54% decrease in Part 5 breaches in this reporting period.

Seven banks, including all four major banks, reported a decrease.

Chart 22: Breaches of Part 5 by Chapter



The overall decrease in Part 5 breaches can be attributed largely to one major bank reporting a 69% decrease – 841 breaches down from 2,686. This bank explained the decrease was primarily due to changes in its quality assurance processes and the way it categorised breaches.

Despite the decrease overall, eight banks reported an increase (although seven had a variance of less than four breaches).

One bank reported a 50% increase on its previous reporting period and cited high volumes of loan variation requests due to changing interest rates as the main reason. The breaches from this bank included failures to act on these requests in a timely manner and errors in processing.

Common breaches of responsible lending obligations based on the breach sample:

- Inadequate credit checks when assessing credit affordability.
- Not verifying the income and liabilities of customers.

Breach sample

The sample data for Part 5 comprised 410 incidents which included 986 breaches. This represents 53% of the total Part 5 breaches.

Of the 410 incidents, 312 contained breaches of Part 5 alone (884 breaches). The remaining 98 incidents included 102 breaches of Part 5 and other Parts of the Code.

These incidents affected 5,180 customers and had a financial impact of $9.9 million.

There were only four breaches of obligations for LMI under Chapter 19.

The sample revealed that the four breaches, reported across three incidents, were due to two banks overcharging. While three of these breaches resulted in no financial or customer impact, the remaining one was reported as having affected 100 customers and had a financial impact of $45,000.

The sample data included 962 breaches of the obligation to have a responsible approach to lending under Chapter 17.

Most of these breaches (93%) were caused by human error, and it is encouraging to see that banks identified this through their own quality assurance processes rather than customer complaints (6%) or the Australian Financial Complaints Authority (AFCA) (1%).

Common errors included:

- Not properly assessing whether a loan or credit card was suitable for a customer.
- Errors when calculating a customer's affordability.
- Not taking reasonable steps to verify a customer’s income and liabilities.
- Not making reasonable enquiries when shown evidence of undisclosed debts.
- Charging fees greater than what was quoted during the loan establishment.
- Applying the incorrect rate to products.

Chart 23: Cause of breaches of Part 5

Chart 24: Identification of breaches of Part 5

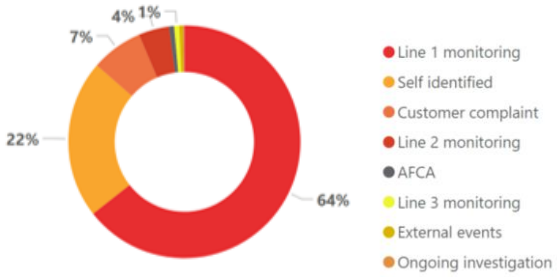


Chart 25: Remediation of breaches of Part 5

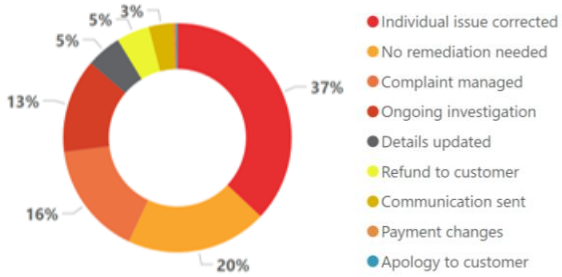


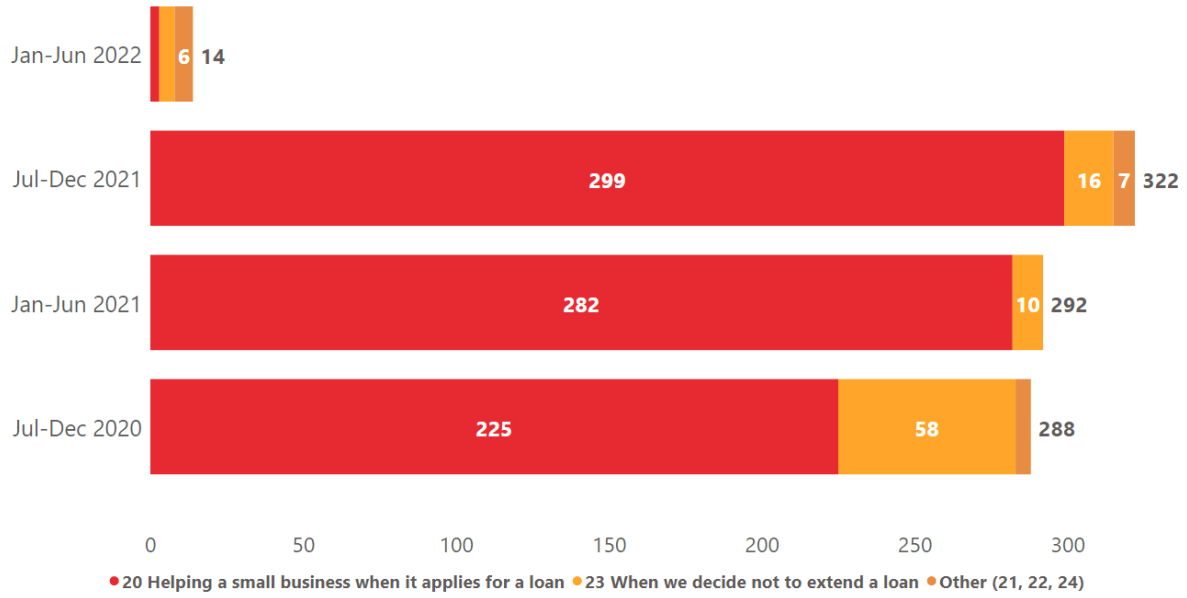
Chart 26: Corrective action taken in response to breaches of Part 5

Part 6 Lending to small business

Part 6 contains obligations for lending to small business customers.

Banks reported a significant decrease of 96% in breaches of Part 6, with only 14 breaches in this reporting period.

Chart 27: Breaches of Part 6 by Chapter



This decrease is mainly the result of one major bank which had reported over 250 breaches for the 2020 and 2021 reporting periods, but only 4 breaches in this period. It cited a change in its approach to the way it classified and reported these breaches as the reason for the decrease.

The very low number of breaches of Part 6 raises concerns about the accuracy of the way banks monitor compliance with the obligations and report on compliance.

The data we received in the most recent six reporting periods shows only 10 banks have reported breaches of Part 6 in one or more reporting periods. The number of breaches reported by nine of those banks is usually less than 10.

The small number of breaches reported by so many banks suggests there may be issues with the controls to monitor, identify and accurately capture breaches of these important obligations. It is imperative that banks maintain accurate record-keeping practices to ensure the accuracy of the breach reporting.

Our Small Business and Agribusiness Advisory Panel has advised that small businesses continue to face a variety of challenges in the current economic climate. We anticipate increasing levels of financial hardship for small businesses.

The need for banks to engage with their small business customers is critical and we believe there is room for improvements in the way they monitor compliance with obligations that affect small businesses.

Breach sample

The sample data for Part 6 comprised 11 incidents, which included 11 breaches. This represents 79% of the total Part 6 breaches.

Of the 11 incidents, nine contained breaches of Part 6 alone (nine breaches). The remaining two incidents included two breaches of Part 6 and other Parts of the Code.

These incidents affected 690 customers and had a financial impact of $14,300.

The sample data revealed common breaches:

- Having incorrect documentation for loans.
- Incorrectly applying fees.
- Failing to provide sufficient notice of decisions not to extend loans.
- Failing to issue letters or incorrectly issuing letters of demand.
- Failing to provide pre-application disclosure documents.
- Failing to communicate the timeframes for outcomes or decisions.

One major bank reported a single breach that affected 276 customers when it failed to provide small business loan applicants with pre-application loan information and the timeframe required for a decision.

This follows similar incidents from this bank in the previous two reporting periods. All three incidents shared the same cause (human error), the same identification method (Line 1 monitoring), and the same corrective action (staff training).

While the bank reported no financial impact for incidents, we expect delays in assessment may reduce opportunities for an applicant and result in indirect financial impacts, as well as non-financial impacts, such as stress.

The repeated nature of this incident raises concerns about the way banks identify and address the root causes of breaches. Banks should consider this incident as an example from which to learn and put in place control interventions to prevent recurring Code breaches.

Chart 28: Causes of breaches of Part 6

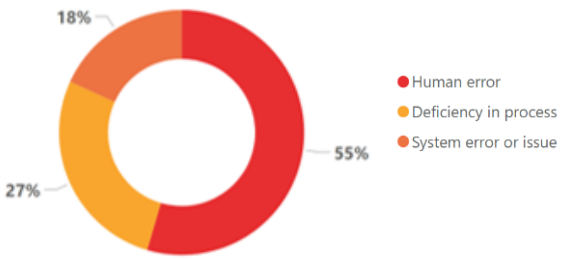


Chart 29: Identification of breaches of Part 6

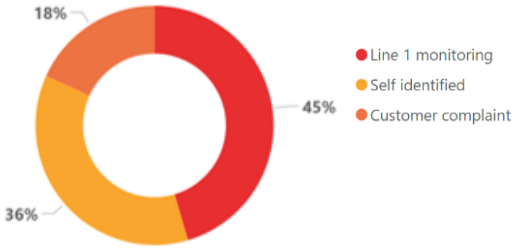


Chart 30: Remediation of breaches of Part 6

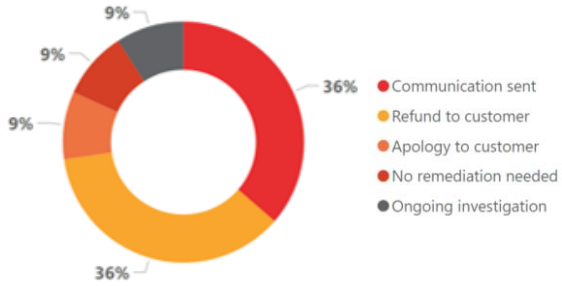
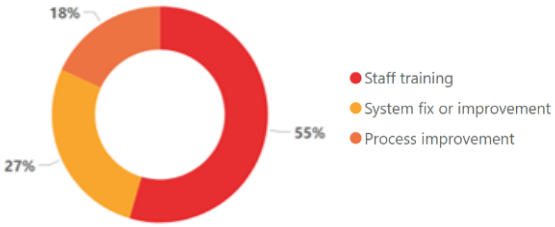


Chart 31: Corrective action taken in response to breaches of Part 6



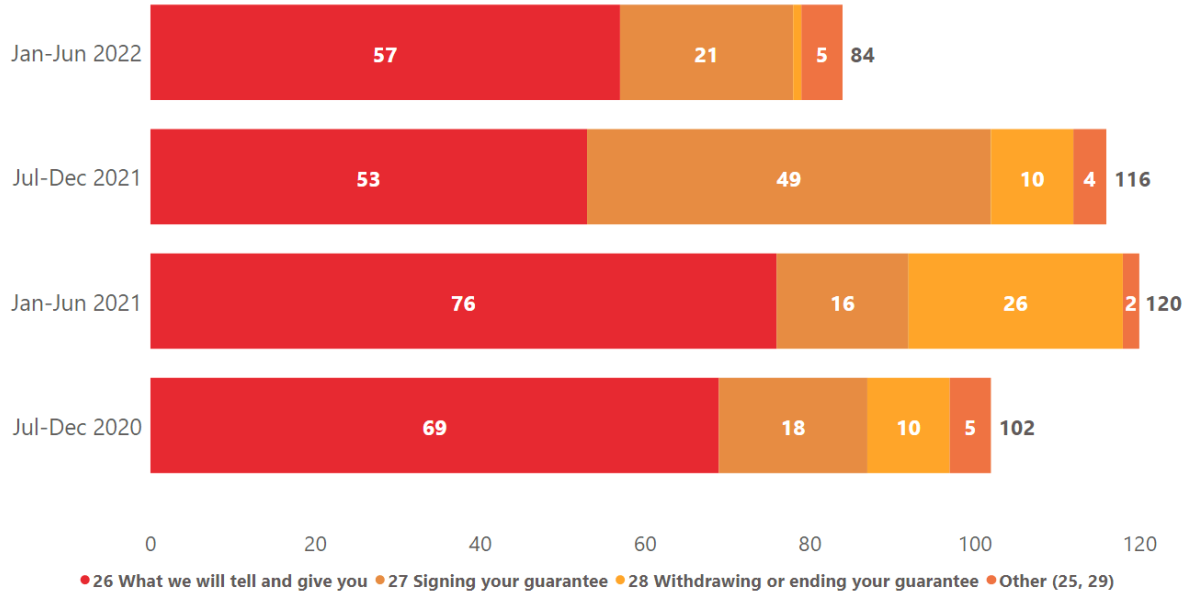
Part 7 Guaranteeing a loan

Part 7 has obligations that work to protect individuals who act as a guarantor for loans.

It outlines the information banks must give prospective guarantors prior to accepting a guarantee. It also sets out requirements for banks for signing, withdrawing or ending a guarantee, and includes conditions for enforcing a guarantee.

In this reporting period, banks reported a 28% decrease in breaches of Part 7.

Chart 32: Breaches of Part 7 by Chapter



Ten banks reported breaches of Part 7, with five reporting an increase and five reporting a decrease compared to the previous period. Only one major bank reported an increase.

Breach sample

The sample data for Part 7 comprised 19 incidents, which included 20 breaches. This sample represents 24% of the total Part 7 breaches.

Of the 19 incidents, 17 contained breaches of Part 7 alone (18 breaches). The remaining two incidents included two breaches of Part 7 and other parts of the Code.

These incidents affected almost 9,771 customers and had a financial impact of $5,400.

We saw a sharp rise in the number of customers affected by breaches of obligations for guaranteeing a loan, with 9,771 affected this period compared to 667 reported in the previous period. However, this is mostly due to a single incident in one bank that had no financial impact.

The incident was a single breach that affected 9,605 customers when it failed to place a required warning notice in its loan documents. The bank corrected the issue and confirmed no customer remediation was required.

Failure to provide relevant documents and disclosures was again the most common breach of Part 7. In this period, it affected 92 customers.

Examples of other breaches of obligations for loan guarantees:

- Failing to provide guarantee documents to a guarantor.
- Failing to ensure the guarantor and borrower execute the documents independently of each other.
- Failing to advise a prospective guarantor to seek independent financial advice.
- Failing to wait until the third day after guarantee documents were issued before accepting the guarantee.
- Failing to provide a timely and useful response when a customer requested to cancel a guarantee.

Human error remained a major source of breaches, accounting for 70% in this period. However, this is a notable decrease from the 82% in the previous period.

Staff identified a greater percentage of breaches in this period, with 55% being a significant rise on the 14% of the previous period.

The Code's guarantee obligations provide important protections to ensure potential guarantors can make fully informed decisions before agreeing to be a guarantor.

Our inquiry report on compliance with the Banking Code's guarantee obligations, published in August 2021, highlighted a number of issues and made 23 recommendations for improved practice and offered practical examples.

We expect the downward trend to continue for breaches of guarantee obligations. Our follow-up inquiry on guarantee obligations will consider how banks have responded to the recommendations in our report and how they have since improved their practices.

Chart 33: Cause of breaches of Part 7

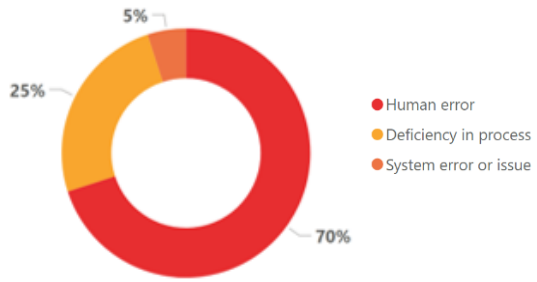


Chart 34: Identification of breaches of Part 7

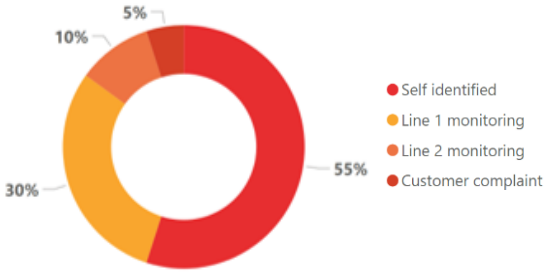


Chart 35: Remediation of breaches of Part 7

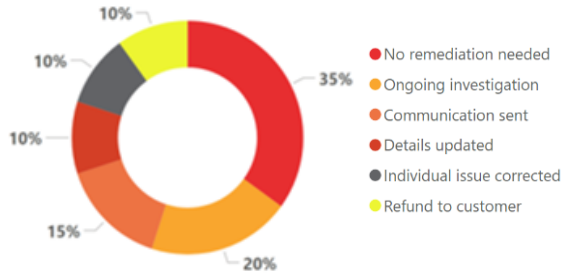
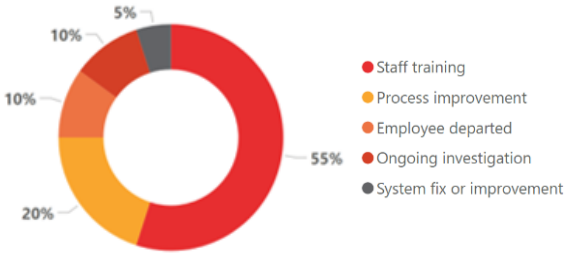


Chart 36: Corrective action taken in response to breaches of Part 7

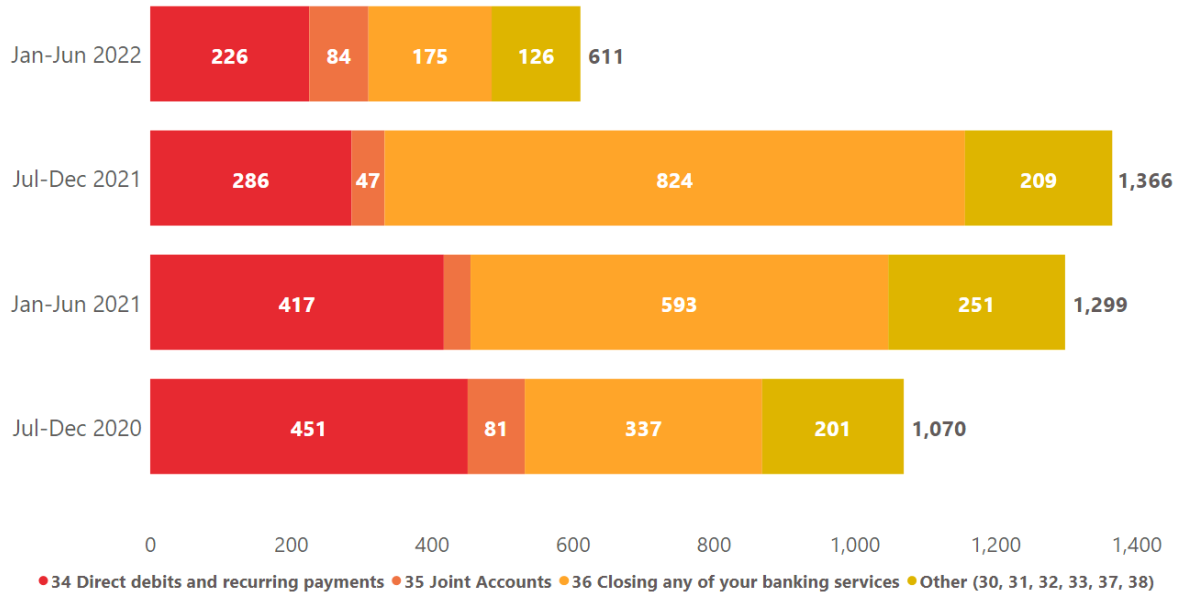


Part 8 Managing your account

Part 8 of the Code covers obligations for transactional banking services.

While collectively there was a large decrease of 55% in breaches of Part 8, only six banks individually reported a decrease in these breaches.

Chart 37: Breaches of Part 8 by Chapter



One major bank reported a significant decrease in breaches compared to the previous period, from 924 down to 59. It attributed this result to a change in its approach to reporting breaches of the Code.

Eleven banks reported an increase in breaches of Part 8 but only two reported an increase of more than 10 breaches. And both banks attributed the increase to changes in their internal identification processes which improved the way they captured breaches.

Breach sample

The sample data for Part 8 comprised 159 incidents, which included 465 breaches. This represents 76% of the total Part 8 breaches.

Of the 159 incidents, 102 contained breaches of Part 8 alone (351 breaches). The remaining 57 incidents included 114 breaches of Part 8 and other Parts of the Code.

These incidents affected 578,995 customers and had a financial impact of $1.6 million.

The sample data revealed the following breaches with higher numbers of affected customers:

Table 7: Breaches with high numbers of affected customers

Breaches	Customers affected
Failing to send notifications that statements are ready to view.	302,140
Processing debit transactions, including interest and fees, after an account was closed.	202,004
Insufficient notice of variation in terms and conditions.	63,067
Failing to return account credit balance to its customers upon account closure in the instances where the account balance was less than $10.	4,548
Customers not receiving account statements.	4,337

Chart 38: Cause of breaches of Part 8

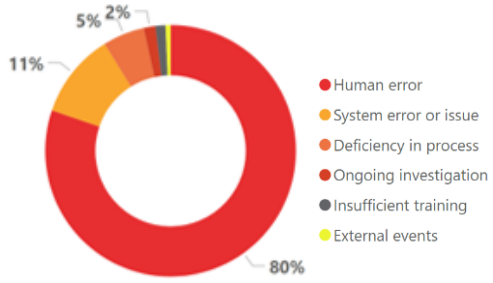


Chart 39: Identification of breaches of Part 8

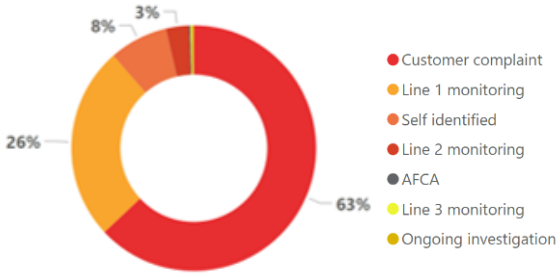


Chart 40: Remediation of breaches of Part 8

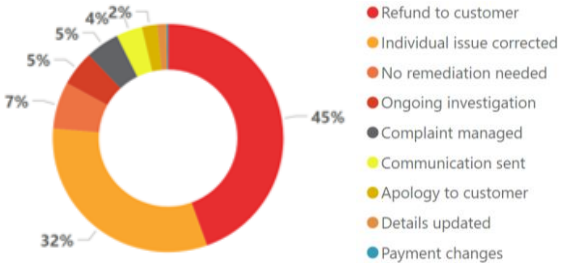
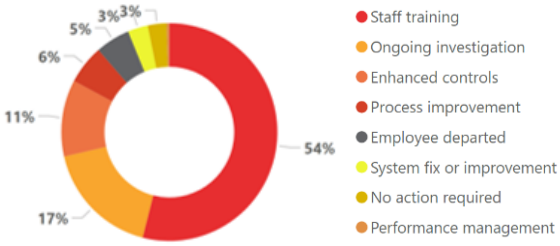


Chart 41: Corrective action taken in response to breaches of Part 8



Part 9 When things go wrong

Part 9 covers obligations for when an individual or small business customer experiences financial difficulty.

The obligations relate to timeframes for dealing with requests for financial difficulty assistance, communications with customers, and a commitment to work with and help customers in financial difficulty.

It also has obligations regarding deceased estates, debt collection and the sale of debts.

SPOTLIGHT – Financial difficulty

Paragraph 157 of the Code defines financial difficulty to mean a customer who is unable to repay what they owe and is experiencing difficulty meeting repayment obligations.

This can be because of an unexpected event or changes outside of their control.

Timely communication

The obligation
Banks commit to respond promptly to requests from customers or their representatives to discuss their financial difficulties.

The bank will reply within the timeframes set by the National Credit Code (NCC) (where applicable).

What we saw
We saw a number of incidents that involved delays in responding to customers experiencing financial difficulty. The examples show that issues with processes were a common cause of delays.

- One major bank failed to respond to 1,068 hardship requests from customers within the required timeframe. This was caused by a range of issues, including a deficiency in its processes, human error and insufficient training.

- One major bank failed to promptly acknowledge the hardship requests or enquiries of 54 customers. Of these, 44 were identified through customer complaints and were caused by human error and 10 were identified through Line 2 monitoring and caused by a deficiency in process. This resulted in financial impact of $112,000.

- One major bank failed to respond to requests for hardship for 247 customers within the required timeframes. This was identified by staff and was caused by a system error.

- One major bank failed to communicate the outcome of hardship requests in a timely manner to 214 customers as required under the NCC. This was due to a deficiency in process.

- One major bank failed to communicate with 183 customers who had open complaints and were experiencing financial difficulty within the required timeframes. This breach was caused by a deficiency in process.

What we expect
It is imperative that banks meet their obligations to customers experiencing financial difficulty. This includes communicating in a clear and timely manner so the customers can make informed decisions about their options.

Timely communication also minimises the risk of exacerbating the stress and vulnerability of difficult circumstances.

Failure to provide customers with the outcome of their financial difficulty request

The obligation
Banks must inform customers in writing of the outcomes of financial difficulty requests, including reasons for the decisions and the main details of the arrangements if they are proposed.

What we saw
- One major bank failed to issue written hardship request outcomes to 265 customers. This was due a system issue that sent accounts with hardship arrangements down an incorrect workflow.

- One major bank failed to provide 221 customers with outcomes to their financial hardship requests due to a system error that allocated the customers to the wrong queue.

- One major bank failed to provide decisions in writing to 138 customers about hardship requests. This was a system error that was identified through line 1 monitoring.

- One bank charged arrears fees to 10,437 home loan accounts that had hardship arrangements. This was due to a deficiency in process that was identified by staff.

What we expect
Banks should prioritise responding to financial difficulty requests from customers and ensure that the outcomes are communicated in writing and in a timely manner.

Contacting customers despite collections activity being put on hold

The obligation
Banks are expected to adhere to the ACCC's and ASIC's Debt Collection Guideline: For Collectors and Creditors when dealing with debt collection activities.

What we saw

- One major bank continued its collection activity with 138 customers while hardship applications were being processed. This was due to a system error.
- One major bank incorrectly issued default notices to 42 customers, including customers on existing hardship arrangements. This was due to both a system error and human error.
- One major bank failed to record the agreed hardship arrangements of 122 customers due to a system issue, resulting in possible collection contacts or escalations.
- One major bank incorrectly reported on the repayment history of 68 customers while they were on a financial hardship arrangement. This was caused by human error and resulted in financial impact of $39,088.
- One bank contacted 1,347 home loan customers about collections by email and SMS on weekends and some public holidays due to a system error.

What we expect
Most of the breaches above were identified though customer complaints. We expect banks to implement proactive measures to detect and prevent these breaches.

Breaches of obligations for financial difficulty and debt collection can have significant effects on customers and may have long term implications.

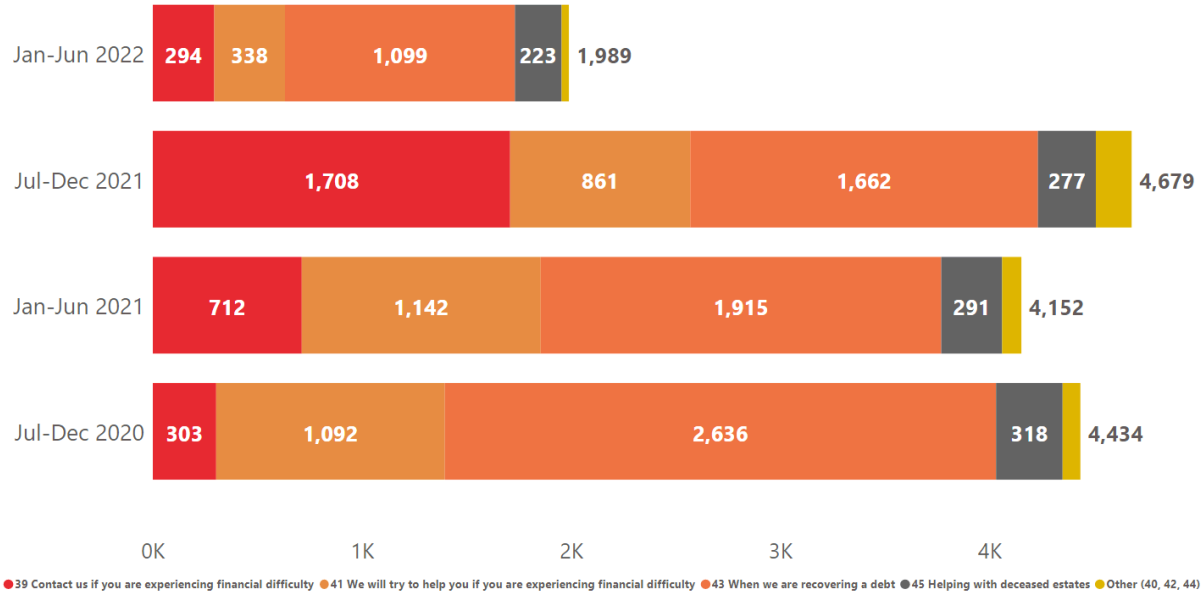
In the current economic climate, there may be an increase in customers experiencing financial hardship, so it is critical that banks do all they can to assist customers.

The majority of the above breaches were corrected by staff training. This suggests a tendency to undertake routine compliance training as remediation rather than to enhance monitoring, fix systems or improve processes.

We encourage banks to carefully consider the corrective action they take and whether it is informed by the root cause of the breach.

We saw a 57% decrease in breaches of Part 9 in this reporting period, an improvement from the 13% increase reported in the previous period.

Chart 42: Breaches of Part 9 by Chapter



Most breaches of Part 9 came under Chapter 43 obligations, followed by obligations for timely action (Chapter 39) and financial difficulty assistance (Chapter 41).

Common breaches based on the breach sample:

- Issuing default notices to customers with financial hardship arrangements.
- Reporting incorrect repayment history information to customers with financial hardship arrangements.
- Failing to maintain accurate records of customer conversations, correspondence or action on debt collection.
- Failing to promptly acknowledge or respond to financial difficulty requests or enquiries.
- Failing to provide customers with outcomes of their financial difficulty requests.

The sample data revealed notable examples of breaches of Chapter 45, which concerns obligations for deceased estates:

- Charging administration fees and failing to waive penalty interest on accounts of deceased customers.
- Charging deceased customers mortgage-related fees.
- Delaying access to accounts of deceased customers and instructions for those accounts.
- Failing to provide representatives with clear and accessible information needed to manage the accounts of deceased customers.
- Failing to provide clear information to representatives to manage recurring payments and direct debits from accounts of deceased customers.

We have conducted a comprehensive inquiry into the breaches of obligations for deceased estates and will publish the findings later this year.

Breach sample

The sample data for Part 9 comprised 342 incidents, which included 1,066 breaches. This represents 54% of the total Part 9 breaches.

Of the 342 incidents, 242 contained breaches of Part 9 alone (947 breaches). The remaining 100 incidents included 119 breaches of Part 9 and other Parts of the Code.

These incidents affected 59,588 customers and had a financial impact of $3.8 million.

More than half of the breaches of Part 9 were identified through customer complaints. Line 1 monitoring accounted for nearly one quarter and 13% were identified by staff.

Banks cited human error as the cause for 81% of breaches of Part 9, and corrective action was mostly staff training.

Chart 43: Cause of breaches of Part 9

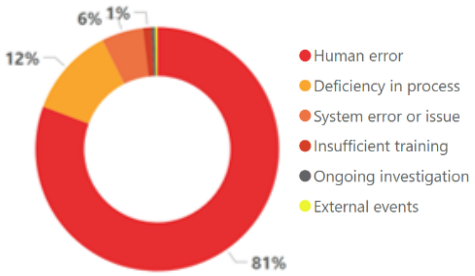


Chart 44: Identification of breaches of Part 9

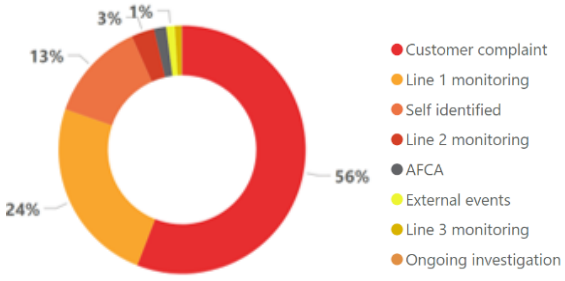


Chart 45: Remediation of breaches of Part 9

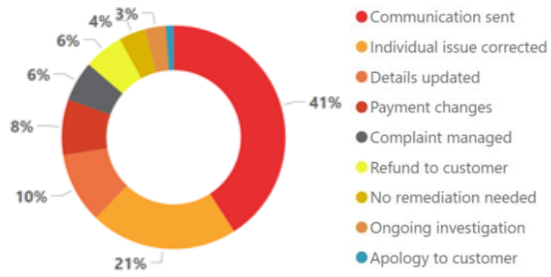


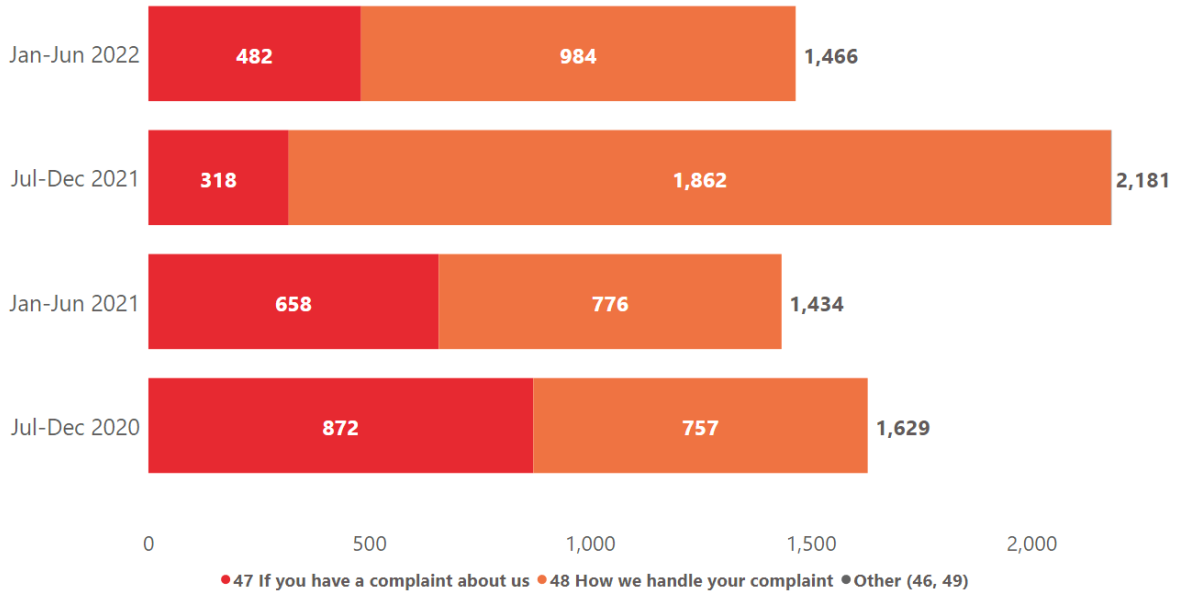
Chart 46: Corrective action taken in response to breaches of Part 9

Part 10 Resolving your complaint

Part 10 sets out how banks should communicate with customers when resolving complaints. It also contains provisions for the role and operation of the BCCC (Chapter 49).

Banks reported a 33% decrease in breaches of Part 10. The breaches only occurred across obligations for complaints (Chapter 47) and how banks handle complaints (Chapter 48).

Chart 47: Breaches of Part 10 by Chapter



Banks attributed the increase in the previous period to the introduction of the ASIC's RG 271, which came into effect on 5 October 2021.

This regulatory guidance updated the requirements for dealing with complaints through an Internal Dispute Resolution (IDR) procedure. It requires financial firms to record all complaints and have an effective system for recording information about complaints.

Given banks were working to meet the updated standards and requirements set by RG271, we anticipated the high number of breaches in the previous period. The subsequent reduction of breaches in this period is a positive development and suggests that the additional compliance measures and integration of changes have been effective.

However, nine banks reported an increase in breaches of Part 10:

- Seven banks reported a slight increase (variance of less than six breaches).
- One major bank reported a 41% increase (510 breaches, up from 362) and attributed it to the introduction of additional measures to identify breaches in line with RG 271.

- One major bank reported a 239% increase (61 breaches, up from 18) and attributed it to a single incident that resulted in multiple breaches. It identified that one of its branches incorrectly captured complaints which affected 40 customers.

The remaining eight banks reported a decrease. The most notable was one major bank that reported a decrease of 64% (473 breaches, down from 1,304). This is the first time this bank reported less than 1,000 breaches of Part 10. The bank attributed the decrease to a range of system updates, process changes and improved capability.

Common breaches of Part 10, Chapter 47, based on sample data:

- Continuing collection activity while customers had open complaints.
- Failing to record complaints.
- Failing to resolve complaints in a timely manner.
- Failing to provide complaint outcomes in a timely manner.
- Failing to include AFCA's details in final letters sent to customers about complaints.

Common breaches of Part 10, Chapter 48, based on sample data:

- Failing to acknowledge complaints within the mandated timeframe.
- Delaying the management of complaints.
- Not resolving complaints within prescribed timeframes.

Breach sample

The sample data for Part 10 comprised 185 incidents, which included 699 breaches. This represents 48% of the total Part 10 breaches.

Of the 185 incidents, 128 contained breaches of Part 10 alone (635 breaches). The remaining 57 incidents included 64 breaches of Part 10 and other Parts of the Code.

These incidents affected 6,574 customers and had a financial impact of $175,000.

Human error remained a major contributor to breaches of Part 10. The majority of breaches caused by human error included:

- continuing collection activity while there was an open complaint
- failing to record complaints or incorrectly recording complaints as feedback
- failing to meet the IDR timelines
- failing to resolve complaints in a timely manner.

Most of the breaches caused by human error were identified by customer complaint (63%) and only 36% were identified by internal sources, such as the three lines of defence process or staff.

In this reporting period, certain system error breaches contributed significantly to the number of customers affected. For instance, a system failure at a major bank resulted in failure to issue SMS receipts of a complaint. This error affected 3,228

customers. In another instance, delays in acknowledging customer complaints from a major bank affected 1,018 customers.

We encourage banks to consider improving internal risk management processes to address the human error and increase capability in detecting non-compliance.

Banks should also consider the new RG 271 requirements and whether they are fully embedded in processes and staff at all levels are aware of and understand them.

Chart 48: Cause of breaches of Part 10

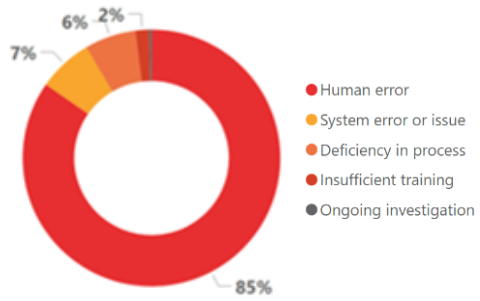


Chart 49: Identification of breaches of Part 10

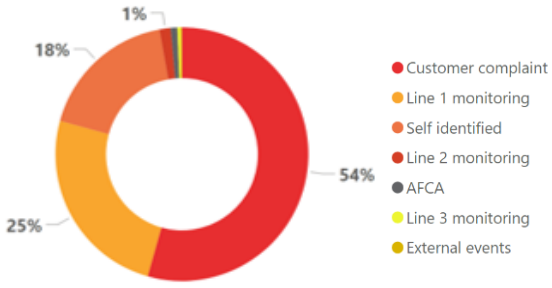


Chart 50: Remediation of breaches of Part 10

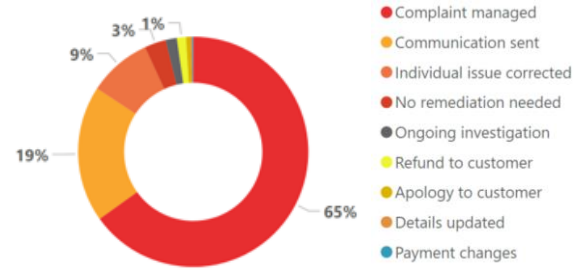
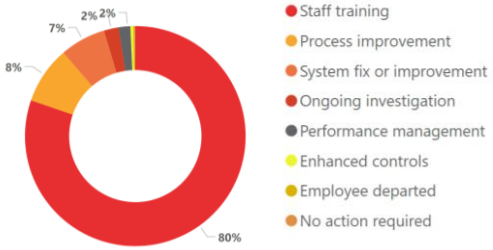


Chart 51: Corrective action taken in response to breaches of Part 10



Appendix

About the BCCC

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 2022–23 Business Plan sets out the priority areas and activities we will undertake to meet the objectives in the Strategic Plan.

Our priority areas for 2022–23 are:

- Guarantees Inquiry Report
- Deceased Estates Inquiry
- issues affecting small business and agri-business customers
- follow up on the Part 4 Report (Vulnerability, Inclusivity and Accessibility)
- implementation of recommendations from the BCCC and Code Reviews.

Our operating procedures provide guidance about how we conduct our monitoring activities. One of the primary ways we monitor banks' compliance with the Code is through the Banking Code Compliance Statement.

Our activities are determined with reference to our Priority Monitoring Framework.

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.