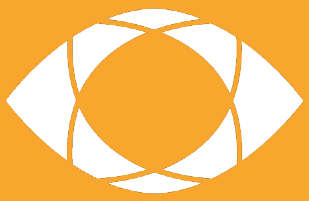


BCCC
Banking Code
Compliance Committee

Banks' compliance with the Banking Code of Practice

July – December 2021

September 2022

Contents

Independent Chair's Message

As Chair of the Banking Code Compliance Committee (BCCC), I am pleased to present our latest report on compliance with the Banking Code of Practice (the Code).

We require subscriber banks to report on their compliance with the Code every six months. This report covers the findings for July to December 2021.

An overall increase in breaches

We saw a 19% increase in breaches from July to December 2021. Banks reported 24,467 breaches in this period, up from 20,605 breaches in the previous six-month period.

The increase was largely driven by Major Bank 4, which had an 86% rise in breaches. It reported 3,973 breaches in this period, up from 2,131 breaches in the previous period.

Major Bank 3 reported a 29% increase, up from 4,054 to 5,231. Major Bank 1 reported a 12% increase, up from 5,935 to 6,664.

These banks largely attributed the increase in breaches to:

- ongoing investment to improve the identification, recording and reporting of breaches
- manual processes relating to COVID packages and hardship applications that are not automated into relevant systems
- challenges in meeting notice and communication inquiries under the Code with the expiry of the COVID-19 Special Note.

Seven other banks also reported increases in breaches this period: Bank A, Bank B, Bank C, Bank D, Bank G, Bank I and Bank J. Although the banks differed this time, there were also seven banks that reported increases in the previous reporting period.

Decrease in breaches for some banks

It was a different story for some, however. One of the major banks and five other banks reported a decrease in breaches for this period.

Major Bank 2 reported a 2% decrease in breaches, coming down from 6,413 to 6,313. This bank attributed the decrease to a simplified operating model, changes in technology and process, and improved understanding of breaches among staff.

Banks E, Bank F, Bank H, Bank L, and Bank M were the others to report decreases in breaches this period.

Our data also found that Bank K reported the same number of breaches this period as it did in the previous period, and Bank N reported no breaches in July to December 2021.

Industry Trends

Fluctuations in breaches

Since the inception of the BCCC and the 2019 Banking Code, the number of breaches reported by banks has fluctuated. In the first half of 2020, banks reported an overall decrease of 5% in breaches. This, however, was overshadowed by the 16% increase in the second half of the year.

We saw a similar result in 2021: the first half of the year saw a 10% decrease in breaches before the second half revealed a 19% increase. With the Code now more than three years old, we would like to see the breaches stabilise in a downward trend, with a greater focus on prevention.

Increased breaches

Most banks attributed the increase in breaches to improved identification and reporting. Banks have been working to improve their compliance frameworks, systems and processes. We know that the improved monitoring has also been prompted by enhanced breach reporting obligations from ASIC.

We welcome banks' ongoing efforts to build their capability to identify and address non-compliance. We expect banks will soon move beyond this consolidation phase with a stronger focus on preventing breaches. This should result in breach numbers coming down over time.

The effect on customers

From July to December 2021, banks provided details for a sample of 3,304 breach incidents.[1] These breaches affected more than 13 million customers[2] and had a financial impact of more than $69 million.[3] In the last reporting period, banks reported 2,803 incidents, which affected more than 2 million customers and resulted in over $56 million in financial impact.

The sample of breach incidents indicates almost 11 million more customers were affected in this reporting period compared to the previous one. And this resulted in an increase of more than $13 million in financial impact.

No doubt the significant regulatory reform of 2021 has played a role here. However, the increase in breaches and the resulting effect on customers demonstrates that there is more work for banks to do.

---

[1] As well as reporting the total number of breaches in a period, banks must provide details of a sample of breaches that met certain criteria.
[2] The number of impacted customers is based on the banks' estimate of the sample of incidents provided for this reporting period. This may include duplication in reporting. For instance, the same customer could be impacted by one or more incidents.
[3] The financial impact is based on the banks' estimate of the sample of incidents provided for this reporting period. This may include financial impact on both the customer and banks.

I encourage all banks to note the feedback we provide them individually – this feedback is a valuable source of guidance on improving compliance with the Code. And just as important are the recommendations and good practice in our inquiry reports, especially the BCCC Building Organisational Capability report.

Impact of COVID-19 on compliance

During this reporting period, a COVID-19 Special Note was in effect, in recognition that the COVID-19 pandemic may affect the timely provision of banking services. The Special Note provided flexibility by exempting reporting of certain timing requirements as breaches. The Special Note was in place during this reporting period from 1 July to 1 September 2021.

Two major banks, out of the 18 banks, reported that they relied on the COVID-19 Special Note in this reporting period. These banks reported incidents that would have ordinarily constituted breaches.

Some banks attributed part of the overall increase in breaches observed during this reporing period to the continued impact of COVID-19 and the expiry of the COVID-19 Special Note. Banks reported an increased volume in COVID-19 packages and hardship applications, followed by further delays and increased complaints due to COVID-19 packages and hardship applications requiring manual tailored solutions.

Furthermore, banks reported higher staff turnover rates due to COVID-19, resulting in errors and increased breaches while new staff were being trained.

Improving data reporting

We continue to engage with the Australian Banking Association (ABA), Australian Securities and Investments Commission (ASIC) and banks on ways to streamline reporting requirements and the guidance needed to improve the consistency and quality of reporting.

We hope to achieve a more consistent approach to breach reporting that will align the reporting capabilities of banks with our monitoring and reporting objectives.

We have developed a comprehensive project plan that will look to address issues of reporting. It will help us to improve the process for banks, resulting in quality data and information and, ultimately, better outcomes for customers.

We are also engaging with ASIC and the Australian Financial Complaints Authority to explore the possibility of increased data sharing. However, this is a long-term project that will take time.

Ian Govey AM
Independent Chairperson
Banking Code Compliance Committee

Introduction

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

One of the primary ways we monitor banks' compliance with the Code is by requiring banks to report breach data in a Banking Code Compliance Statement (Compliance Statement).

The Compliance Statement enables us to:

- benchmark banks' 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.

This report summarises banks' Code breach data for the reporting period from July to December 2021.

The data in this report has been de-identified. All bank names are replaced by placeholders, such as 'Bank A', except for the largest four banks which are referred to as 'Major Bank'.

We have classified and reported on the breach data by reference to which 'Part' of the Code the incident or breach most clearly aligned with and included a more detailed examination of specific Chapters where necessary.

Banks are required to report the total number of breaches they identified during the reporting period, and further details of a sample of breach incidents that met certain criteria.

We require banks to report the details of breaches by describing an incident, event or action and then listing one or more Code obligations that had been breached as a result.

As a result, the number of breaches (or incidents) referred to under each section of the report may not match the total number of breaches reported. Further details can be found in each section. As an example, if one bank reported 1,000 total breaches for the period, it may provide further details of 100 incidents which account for 300 breaches.

We have also included de-identified examples based on individual breaches where the incident is of interest or concern.

Further information about us and the Compliance Statement can be found in **Appendix 1**.

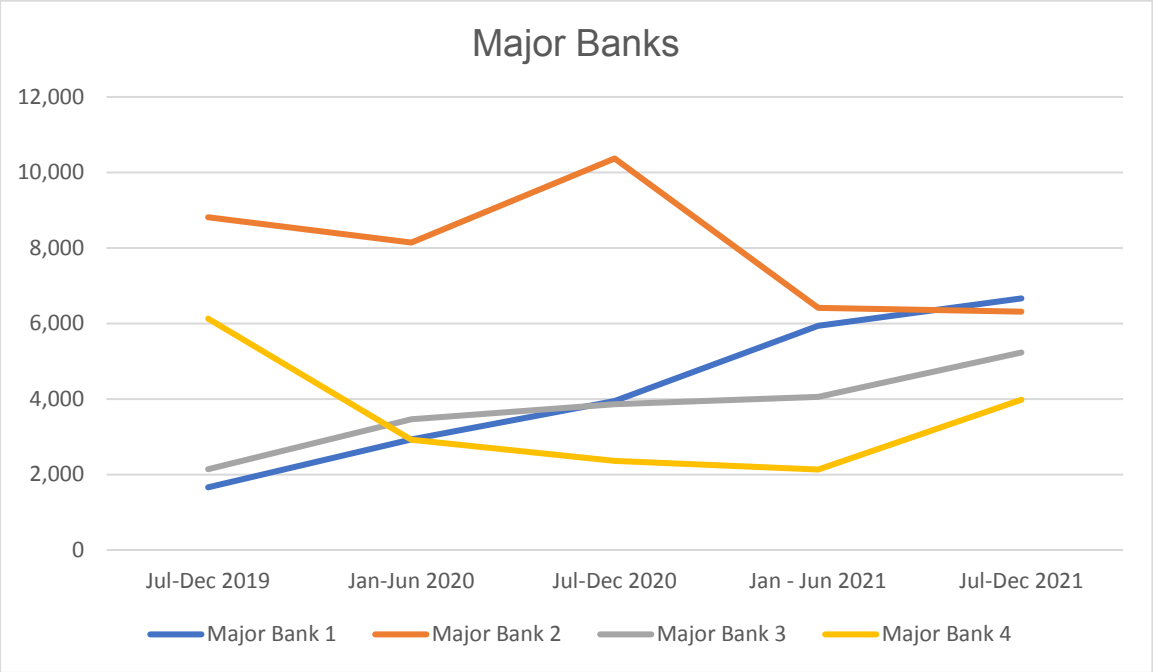
Summary of breaches

Eighteen subscriber banks[4] reported 24,467 breaches of the Code - a 19% increase from the previous six months.

We have been collecting Part A compliance data since our inception in July 2019 for over three years now. The data shows the number of breaches reported by banks has fluctuated over the last four reporting periods.

The four major banks account for 91% of all breaches reported. Three out of four major banks reported an increase in breaches for this reporting period.

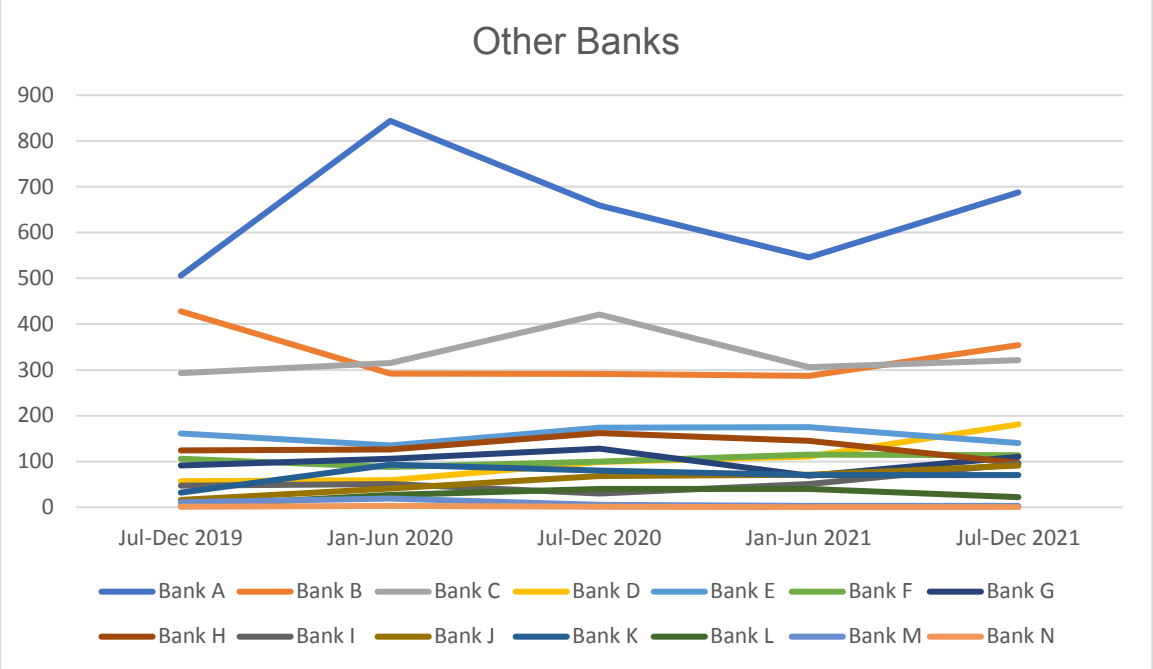
Chart 1: Total number of Code breaches, By Major Banks, July 2019 to December 2021



Over the last four reporting periods inclusive of this one, Major Bank 1 and Major Bank 3 have reported an increase in breaches for each period. Major Bank 4 has reported a decrease over the last three reporting periods but an increase in this reporting period. Major Bank 2 breaches appear to be on a downward trend, having reported a decrease in the last two reporting periods.

[4] We had one less subscribing bank during this reporting period due to relinquishing its membership with the ABA upon its acquisition by another subscribing bank. As a result, there will be one less de-identifier in our charts and tables compared to the last reporting period.

Chart 2: Total number of Code breaches, By Other Banks, July 2019 to December 2021



Bank A, Bank B, Bank C and Bank G reported an increase in breaches in this reporting period compared with a decrease in breaches in the last reporting period.

Banks D and Bank J have reported an increase in all four reporting periods. Bank I has reported an increase in breaches in the last two reporting periods inclusive of this reporting period. Bank E, Bank H and Bank F have reported breaches fluctuating between increases and decreases over the last four reporting periods ending in a decrease in breaches in this reporting period.

Bank L and Bank M have reported the same number of breaches for the previous two reporting periods, while reporting an over 40% decrease in breaches in this reporting period. Bank K has reported the same number of breaches for the last two reporting periods including this period. Bank N reported no breaches for the last two reporting periods inclusive of this reporting period.

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 of a customer's banking experience or for a specific type of customer.

Table 1: Number of breaches, by Code 'Part'

Code Part	Jan to Jun 2021		Jul to Dec 2021	
Part 2 Your banking relationship	7,139	↓ 19%	7,124	↓ <1%
Part 9 When things go wrong	4,152	↓ 6%	4,679	↑ 13%
Part 5 When you apply for a loan	2,076	↓ 28%	3,981	↑ 92%
Part 3 Opening an account and using our banking services	3,442	↑ 12%	3,445	↑ <1%
Part 10 Resolving your complaint	1,434	↓ 12%	2,181	↑ 52%
Part 8 Managing your account	1,299	↑ 21%	1,366	↑ 5%
Part 4 Inclusive and accessible banking	651	↑ 9%	1,249	↑ 92%
Part 6 Lending to small business	292	↑ 1%	322	↑ 10%
Part 7 Guaranteeing a loan	120	↑ 18%	116	↓ 3%
Part 1 How the Code works	0	↓ 100%	2	↑ 200%
Total	**20,605**	**↓ 10%**	**24,467**[5]	**↑ 19%**

Significant movements

The top four Code part breaches for this reporting period, from highest to lowest, are Parts 2, 9, 5 and 3. A slight change of order compared to the previous period, when it was Parts 2, 9, 3 and 5.

There have been significant increases of Parts 4 and 5 breaches in this reporting period compared to the previous period. Breaches of Part 4, relating to inclusive and accessible banking, have increased by 92% compared to the 9% increase in the last reporting period.

[5] One bank reported two breaches of the two previous Codes – the 2013 and 2004 Banking Code of Practice. While these two breaches are not reflected in the Code Part description in the Chart above, it is included in the total number of breaches for this reporting period, Jul to Dec 2021.

Banks explained that the majority of Part 4 breaches relate to:

- banks' failure to appropriately remove or amend account accesses for protected persons upon receipt of a Financial Management Order or a Power of Attorney
- call centre staff not identifying customers who may be experiencing vulnerable circumstances
- staff not confirming with customers whether they hold an eligible Government concession or pension card.

Banks attributed the increased identification of breaches to the introduction of new controls designed to strengthen assurance activities such as an enhanced internal control for review and monitoring of sampled customer conversations.

This increase in reporting may, at least in part, be attributed to our Inquiry into banks' compliance with Part 4 of the Banking Code, focusing on inclusivity, accessibility and vulnerability. Banks are more aware of their Part 4 obligations and appear to be proactively identifying and reporting these breaches to us.

However, it's critical that banks address and reduce Part 4 breaches as a priority to reduce potential harm to customers experiencing vulnerability.

Breaches of Part 5, relating to bank obligations in approving loans, have increased by 92% compared with the 28% decrease in the last reporting period.

One major bank attributed the increase to changes in process and their interpretation of internal obligations, implemented to comply with ASIC Regulatory Guide 78. These changes resulted in different event classifications and proactive identification, investigation and recording of more breaches by Line 1 monitoring teams.

Another major bank explained complicated and lengthy sales guidelines contributed to most of its Part 5 breaches. The bank piloted a simplified sales process that resulted in significant improvements and aims to roll out this process to the wider bank.

Statistics used in this report

In accordance with our reporting instructions (see **Appendix 1**), banks provided further information about the nature, cause, impact and correction of 3,304 incidents, constituting 8,590 breaches – 35% of the total reported. The rest of this section of the report refers only to this subset of incidents.

Cause of breaches

The predominant cause of the incidents reported by the banks remains the same as the previous reporting period (human error – 73% of incidents).

We encourage banks to continue to incorporate sufficient measures into their compliance frameworks to prevent human error related breaches from recurring.

Breach identification

Banks identified 33% of incidents through customer complaint, query or feedback. A further 33% were self-reported by staff and/or immediate managers. 'Line 1' quality assurance activities including call monitoring and system monitoring detected 25% of incidents.[6]

Less than 1% of incidents were identified by Line 2 (internal reviews) and 3% by Line 3 or (internal audits) defences.

Impact

Overall the sample of incidents reported for July to December 2021 affected more than 13 million customers, with a total financial impact of over $69 million. In the previous period, over 2 million customers were affected with a total financial impact of over $56 million.

This increase was largely driven by three banks reporting seven incidents, which resulted in nine breaches impacting over 10 million customers. The banks reported that these breaches were mainly the result of human error, deficiencies in processes and procedures, and system errors or failures.

Customer remediation and corrective actions

We collect data about how banks prevent the recurrence of breaches and the steps taken to remediate the impact of breaches on customers.

To prevent recurrence, the most common actions taken by banks were one or more of the following:

- provided staff training, coaching or feedback (63% of incidents)
- reviewed and/or improved processes (13%)
- implemented a system fix (5%)
- reviewed staff performance or taken disciplinary action (3%)
- enhanced monitoring or controls (3%).

Banks' actions designed to prevent recurrence were still under review at the time of reporting for 9% of incidents. Banks reported that they did not take actions to prevent recurrence or no action was required for approximately 5% of incidents.[7]

Human error remains the predominant cause of breach and it appears banks still overly rely upon staff training as a corrective action. As highlighted in our previous report, better trained staff make fewer errors, but improved systems, processes and controls are key to decreasing the risk of Code breaches and other errors.

[6] Refer to Appendix 1 for more information about the 'three lines of defence'.
[7] Data may not total 100% because banks may have taken one or more of the actions listed.

To address breach impacts on individual customers, banks reported that they had undertaken one or more of the following actions:

- corrected the individual issue, including updating details, and requests for information be destroyed, deleted or returned (41% of incidents)
- provided financial remediation such as a refund, debt waiver, compensation or goodwill payment (25%)
- communicated or corresponded with the customer (7%)
- logged, managed or resolved a complaint (3%)
- apologised to the customer (1%).

Banks reported customer remediation was not required for 9% of incidents. For 12% of incidents, the matter was still under investigation at the time of reporting or the bank had yet to consider customer remediation.

Banks did not provide details of remediation activities for less than 1% of incidents. While we commend banks for responding to our feedback on this issue, we would like banks to provide more complete information in their reporting.

COVID-19 Special Note

In 2020, ABA made temporary changes to the Code to reflect the fact that the COVID-19 pandemic may affect the timely provision of banking services. The ASIC approved these temporary changes.

These temporary changes were annexed to the Code as the COVID-19 Special Note (Special Note) and was in operation initially from 1 July 2020 to 1 March 2021 and later extended to 1 September 2021.

While the Special Note was in place, incidents that would ordinarily constitute breaches in relation to certain timing requirements were exempted. Banks were still asked to provide information about these incidents to the BCCC. However, while the Special Note was in place, these incidents were not considered breaches. The relevant timing requirements under the Code were:

- 101(b)&(c) and 102 – requirements to provide guarantors with information within 14 days about a borrower's deteriorating financial position
- 148 – providing copies of documents within 30 days
- 164 – responding promptly to requests to discuss financial difficulties
- 205 and 206 – complaints handling timeframes.

The Special Note applied to part of this reporting period, 1 July to 1 September 2021 . Two major banks, Major Bank 1 and Major Bank 4, reported incidents under the Special Note in relation to Part 9 – *When things go wrong*. These were not recorded as breaches for the purpose of this report.

The banks attributed these incidents to:

- not meeting the timeframe outlined in the National Credit Code (NCC) to respond to customers' requests for hardship assistance
- delays in front line staff referring hardship notice to the bank's financial hardship team
- individual hardship requests were incorrectly actioned due to human error.

Despite the Special Note being in place for part of this reporting period, banks reported a 13% increase in breaches relating to Part 9. This resulted in breaches related to Part 9 being the second highest for breaches in this reporting period.

Review of the consistency of breach reporting

The quality and consistency of breach reporting has been an important topic of discussion over the last few years for both us and the banks. The quality of the breach data provided by banks impacts our ability to assess if banks are compliant with the Code. Consistent breach reporting from banks enhances the comparability analysis and value of the breach data provided. This allows us to identify what is good practice and, to the extent practicable, how banks compare.

We issued the updated Compliance Statement (Part A) to banks in June 2022 – implementing the changes proposed as part of the consultation on breach categories. We look forward to receiving the banks' submission of the updated compliance statement in September 2022.

As mentioned in our Chair's message, we are committed to investing in our overall data collection and analytics capabilities in the hope of aligning banks' reporting capabilities with our reporting and monitoring objectives.

Banks' compliance with the Banking Code

We have classified and reported on the breach data by reference to which 'Part' of the Code the incident or breach most clearly aligns with and included a more detailed examination of specific chapters and sections where necessary.

Part 2 – Your Banking Relationship

Banks reported 7,124 breaches overall of Part 2, making it the Code Part with the highest breaches in this reporting period.

Table 2: Breakdown of Part 2 Code breaches, By Chapter

Chapter	Jan-Jun 2021	Jul-Dec 2021	% change
3 Our compliance with this code	0	5	↑ 500%
4 Trained and competent staff	2,474	2,754	↑ 11%
5 Protecting confidentiality	4,662	4,349	↓ 7%
6 Compliance with laws	1	13	↑ 1,200%
7 Closing a branch	2	3	↑ 50%
Total	**7,139**	**7,124**	**↓ <1%**

Chapter 4 – Trained and competent staff

Chapter 4 includes two important obligations - to have trained and competent staff and that staff will engage with customers in a fair, reasonable and ethical manner.

Banks reported a 11% increase in Chapter 4 breaches compared with a 46% decrease reported in the last reporting period.

Banks' sample

Banks provided further information on 894 incidents, constituting 1,330 breaches and impacting more than 900,000 customers.

Three major banks accounted for 94% of the customers impacted by Chapter 4 breaches and attributed the breaches to process deficiency and system failure. Incidents reported by banks included:

- incorrectly charging customers interest and/or fees
- reporting incorrect information on customers' credit file
- providing incorrect information to customers about their financial product.

Banks' reported 60% of these incidents were caused by human error – a 4% decrease from the last reporting period, followed by process deficiencies and system failures. Banks' corrective action in 46% of these incidents was staff training and feedback.

It appears that banks may still be blaming human error for breaches where better systems may have prevented staff from making the error and over-relying on staff training and feedback to prevent recurrence of human error where improvements to systems and controls might be more effective.

We encourage banks to:

- conduct proper root cause analysis to identify the real cause(s) behind an incident or breach
- uplift their systems, processes and controls to prevent breaches and reduce the possibility of human error.

Chapter 5 – Protecting Confidentiality

Chapter 5 includes obligations regarding privacy and confidentiality. Each year privacy and confidentiality breaches account for the highest or second highest category of reported breaches. This trend has continued with 4,349 breaches reported for this period, making Chapter 5 the highest category of reported breaches.

Breaches of privacy provisions are of ongoing concern to us and can be serious in nature, with considerable impact on customers, such as:

- unauthorised access to customers' accounts by criminals
- incorrect account access by POA holders or executors and family members
- customers' contact details and addresses being disclosed to abusive ex-partners.

The improvements in Chapter 5 breaches are not being seen across the board. For instance, two of the major banks have shown a decrease in the number of breaches, while the other two major banks show an increase in these breaches.

Banks' sample

Banks provided further information on 793 incidents, constituting 1,415 breaches and impacting more than 4 million customers.

Major Bank 2 accounted for 98% of the customers impacted and it reported that the majority of the breaches were manual errors made by its front-line staff.

Major Bank 2 acknowledges that Chapter 5 continues to be an area that requires improved compliance and expects to do this by enhancing its privacy framework. To reduce manual errors, it is simplifying and automating some of its processes and delivering targeted training. Major Bank 2 also highlighted that it has recruited a significant number of frontline staff during this reporting period.

Part 3 – Opening an account and using banking services

Part 3 of the Code (Chapters 8 to 12) specifies how banks will communicate with customers and that information provided will be clear. It also contains specific requirements about the contents of terms and conditions.

Banks reported 3,445 breaches of Part 3 and 88% of the breaches were reported by major banks.

Table 4: Breakdown of Part 3 Code breaches, By Chapter

Chapter	Jan-June 2021	Jul-Dec 2021	% change
8 Providing you with information	955	888	↓ 7%
9 Communication between us and you	1,506	1,622	↑ 8%
10 Responding to your request for information	115	84	↓ 27%
11 What information we will give you	739	729	↓ 1%
12 Acquiring a new product or service	127	122	↓ 4%
Total	**3,442**	**3,445**	**↑ <1%**

The decrease in Chapter 10 breaches is largely attributed to a reduction of breaches reported by Major bank 3, which has reported 57% fewer breaches than the previous reporting period. The bank explained that it has refined their approach to categorising breaches since the last reporting period. This has contributed to fluctuations in breaches being reported under Part 3 obligations.

Major Bank 1 reported 900 breaches related to Chapter 9 obligations. This is a 35% increase from the previous reporting period and accounts for 55% of the total Chapter 9 breaches. The bank explained that the increase in breaches was due to delays in processing loan disputes.

Major Bank 2 reported a 286% increase in Chapter 8 and a 40% increase in Chapter 11 breaches. The bank reported that the majority of the breaches related to staff failing to advise customers of applicable fees when switching products and failing to provide disclosure information where required. It further explained that the increased identification of breaches can be attributed to a combination of a high number of new staff, and the introduction of enhanced controls and monitoring.

Banks' sample

Banks provided further information on 554 incidents, constituting 1,039 breaches and impacting more than 8.3 million customers.

Bank I and Bank F have reported three incidents (five breaches) that collectively affected 7.3 million customers. These breaches were related to Chapter 8 and 9 obligations and were generally related to communications being sent using the wrong contact channel and banks providing outdated terms and conditions or insufficient disclosures. Two of those incidents were corrected through implementing process improvements and remediating customers, while

one incident affecting 3.3 million customers of Bank F was under investigation at the time of reporting.

Banks reported that 66% of the incidents were the result of human error, 16% involved a deficient process or procedure and 13% related to a system issue or error.

Banks identified 34% of Part 3 incidents through customer complaints, 33% self-identified or reported by a staff member and 26% via first line monitoring.

Banks provided financial remediation to customers for 31% of the incidents. Banks' corrective actions to prevent further breaches were predominantly through staff training, coaching or feedback - 54% of the incidents.

Part 4 – Inclusive and accessible banking

Part 4 of the Code (Chapters 13 to 16) includes banks' obligations to provide inclusive and accessible banking services, including accounts and services for people on a low income, and taking extra care with customers who may be experiencing vulnerability.

Banks reported 1,249 breaches of Part 4 for this period – a 92% increase from the previous six months. Seven banks reported no breaches.

Table 5: Breakdown of Part 4 Code breaches, By Chapter

Chapter	Jan-June 2021	Jul-Dec 2021	% change
13 Being inclusive and accessible	29	67	↑ 131%
14 Taking extra care with customers who are experiencing vulnerability	398	843	↑ 112%
15 Banking services for people with a low income	201	290	↑ 44%
16 Basic accounts or low or no fee accounts	23	49	↑ 113%
Total	**651**	**1,249**	**↑ 92%**

Major Bank 2 reported a 340% increase in Part 4 breaches – accounting for half of the breaches reported under Part 4 of the Code.

Major Bank 2 reported a 341% increase under Chapter 14 and a further 240% increase under Chapter 15 of the Code, collectively accounting for 96% of the total Part 4 breaches identified by the bank. The bank attributed the increased identification of breaches to the introduction of new controls which have strengthened assurance activities.

Banks' sample

Banks provided further information on 120 incidents, constituting 172 breaches and impacting more than 4,000 customers.

The majority of impacted customers can be attributed to three incidents (three breaches) related to Chapter 16 obligations, which were reported by Major Bank 1, Major Bank 2 and Bank C. These three incidents were generally in relation to incorrect fees being charged or over-drawing of basic accounts and collectively impacted 3,757 customers. The banks have confirmed that the incidents have been corrected through implementing process or system improvements, enhancing monitoring or controls, and remediating customers.

Overall, the nature of the incidents banks reported remains the same as in the previous reporting period including:

- failure to identify and take extra care with customers who may be experiencing vulnerability
- customers on low incomes are not offered no-fee accounts

- failure to take extra care with vulnerable customers who are subjected to scams or fraud
- errors made in dealing with a Power of Attorney and account processing issues.

Banks identified 88% of the incidents were caused by human error, 5% by a deficient process and procedure and 3% by a system issue or error. Significantly, there is a 15% increase in human error related incidents in this period.

38% of incidents were self-identified or reported by a staff member, 34% through customer complaints and 24% by Line 1 monitoring.

Banks provided financial remediation to customers for 34% of these incidents. Banks' corrective actions to prevent further breaches were predominantly through staff training, coaching or feedback - 75% of the incidents.

Part 5 – When you apply for a loan

Part 5 of the Code (Chapters 17 to 19) contains the provisions relating to responsible lending.

Banks reported 3,981 breaches of Part 5, making it the Code Part with the third highest breaches in this reporting period.

Table 6: Breakdown of Part 5 Code breaches, By Chapter

Chapter	Jan-Jun 2021	Jul-Dec 2021	% change
17 A responsible approach to lending	1,987	3,852	↑ 94%
18 Our approach to selling consumer credit insurance (CCI)	86	121	↑ 41%
19 Lenders mortgage insurance	3	8	↑ 167%
Total	**2,076**	**3,981**	**↑ 92%**

As seen from the above table, nearly all Part 5 breaches are of Chapter 17, with breaches of the other chapters being low. Chapter 17 requires banks to undertake a responsible approach to lending to individuals and small businesses.

Banks reported a 94% increase in Chapter 17 breaches compared with a 31% decrease reported in the last reporting period. The increase was largely driven by Major Bank 4, which had a 215% rise in Chapter 17 breaches in the last reporting period.

In this period, Major Bank 4 accounted for 70% of Chapter 17 breaches and the other major banks collectively accounted for 28%. Six banks did not report any breaches of Chapter 17.

Major Bank 4 explained that the increase in Chapter 17 breaches was a result of changes to the bank's internal quality assurance processes ahead of the commencement of ASIC's breach reporting regime in October 2021 and represent processing issues identified and corrected by the bank. Due to the changes in the bank's quality assurance processes, the vast majority of these breaches resulted in no financial detriment and were rectified with limited or no customer involvement.

Banks' sample

Banks provided further information on 307 incidents, constituting 735 breaches and impacting more than 9,000 customers.

Banks reported that 76% of the incidents were the result of human error, 10% related to deficient processes or procedures and 6% related to a system issue or error. While human error remains to be the predominant cause of the breaches, the sample shows system error and deficiencies in processes/procedures resulted in the highest customer impact. Banks identified:

- 18 incidents with system errors which impacted approximately 6,530 customers
- 30 incidents with deficiencies in processes and procedures which impacted approximately 1,470 customers.

Part 6 – Lending to Small Business

Part 6 of the Code (Chapters 20 to 24) contains banks' obligations when lending to small business customers.

Banks reported 322 breaches of Part 6 for this period – a 10% increase from the last reporting period. Only six banks reported breaches under Part 6 in this period.

Table 7: Breakdown of Part 6 Code breaches, By Chapter

Chapter	Jan-Jun 2021	Jul-Dec 2021	% change
20 Helping a small business when it applies for a loan	282	299	↑ 6%
21 When will we not enforce a loan against a small business	0	1	↑ 100%
22 Specific events of non-monetary defaults	0	1	↑ 100%
23 When we decide not to extend a loan	10	16	↑ 60%
24 When we appoint property valuers, investigative accountants and insolvency practitioners	0	5	↑ 500
Total	**292**	**322**	**↑ 10%**

Major Bank 3 accounted for 91% (292 breaches) of Part 6 breaches. This is a 5% increase from the previous reporting period (279 breaches). Bank A accounted for 6% of Part 6 breaches. Bank A reported a 111% increase in Part 6 breaches compared with the previous reporting period.

Banks' sample

Banks provided further information on 16 incidents, constituting 306 breaches and impacting approximately 801 customers.

One of the incidents, where pre-application disclosure documents were not provided and the timeframe required for outcome/decision was not communicated, affected 304 small business customers. This incident was reported as 287 separate breaches of Chapter 20.

The same bank reported a breach where it failed to issue a notice of its decision not to extend a loan. This breach impacted approximately 416 small business customers. The matter was still under investigation at the time of reporting and the bank had yet to complete customer remediation.

Part 7 – Guaranteeing a loan

Part 7 of the Code (Chapters 25 to 29) encompasses the obligations for guaranteeing a loan such as a guarantor's right to limit or end a guarantee, and banks' obligations to provide important notices and any adverse credit information about the borrower's financial position.

Banks reported a 3% decrease in breaches of guarantee provisions for this reporting period – an improvement from the 18% increase that was reported in the last reporting period.

Table 9: Breakdown of Part 7 Code breaches, By Chapter

Chapter	Jan-Jun 2021	Jul-Dec 2021	% change
25 Limiting liability under the guarantee	2	4	↑ 100%
26 What we will tell and give you	76	53	↓ 30%
27 Signing your guarantee	16	49	↑ 206%
28 Withdrawing or ending your guarantee	26	10	↓ 62%
29 Enforcing your rights under the guarantee	0	0	-
Total	**120**	**116**	**↓ 3%**

One major bank accounted for 100% of breaches reported under Chapter 25. The four major banks accounted for 81% of breaches reported under Chapter 26 and 96% of the breaches reported under Chapter 27.

Major Bank 1 accounted for 55% of breaches reported under Chapter 27. This bank did not provide further information about the incidents related to these breaches because it did not trigger the criteria in question two of the compliance statement.

Banks' sample

Banks provided further information on 24 incidents, constituting 41 breaches and impacting more than 500 customers.

Incidents reported by banks remain the same as the previous reporting periods. These included:

- not providing the three-day period before the signing of a guarantee
- incorrect or incomplete information being provided to guarantor
- failure to end guarantees.

Banks reported that 75% of the incidents were the result of human error, 54% were identified through Line 1 monitoring activities and corrected though staff training, coaching or feedback.

Guarantees remain a priority focus area for us. In August 2021, we published our Guarantees Inquiry report, noting concerns about effective record management practices, inadequate or ineffective monitoring of compliance controls and guarantee-related data capabilities.

We commenced a follow up Inquiry on Guarantees last month.

Part 8 – Managing your account

Part 8 of the Code (Chapters 30 to 38) largely covers obligations about day to day transactional banking services. Banks reported a 5% increase of Part 8 breaches for this reporting period compared to the 21% increase reported in the last reporting period.

Table 10: Breakdown of Part 8 Code breaches, by Chapter

Chapter	Jan-Jun 2021	Jul-Dec 2021	% change
30 Keeping your accounts safe and secure	19	14	↓ 26%
31 Statements we will send you	46	22	↓ 52%
32 Cost of transaction service fees	17	12	↓ 29%
33 Managing a credit card	41	20	↓ 51%
34 Direct debits and recurring payments	417	286	↓ 31%
35 Joint Accounts	38	47	↑ 24%
36 Closing any of your banking services	593	824	↑ 39%
37 Your right to copies of certain documents	49	87	↑ 78%
38 When we change our arrangements with you	79	54	↓ 32%
Total	**1,299**	**1,366**	**↑ 5%**

Breaches reported for Chapter 30, 32, 33, and 34 appear to be on a downward trend. Banks reported a decrease for these chapters in the current and previous reporting periods.

In contrast, number of breaches reported under Chapter 36 has been increasing since January 2020. In the all four periods inclusive of current period, Major Bank 1 continues to account for the majority of Chapter 36 breaches. In this period, Major Bank 1 accounted for 79% for Chapter 36 breaches. Major Bank 1 explained that the increase in this period was related to credit cards and direct debits.

In the last and current reporting periods, Major Bank 2 and Major Bank 3 reported a decrease in their Part 8 breaches. In both periods, they collectively accounted for less than 18% of Part 8 breaches.

Banks' sample

Banks provided further information on 134 incidents, constituting 435 breaches and impacting more than 63,000 customers.

Banks reported that 71% of the incidents were the result of human error and its corrective actions to prevent further breaches were predominantly through staff training, coaching or feedback (67%). Banks identified 44% of incidents through customer complaints and resolved the breaches primarily by issuing a refund/reimbursement/goodwill payment (36%). We saw a similar trend with slight percentage difference, in the sample provided for the last reporting period.

Part 9 – When things go wrong

Part 9 of the Code (Chapters 39 – 45) contains obligations on banks to assist customers experiencing financial difficulty. These provisions 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. Part 9 also contains provisions regarding deceased estates, debt collection and the sale of debts.

Banks reported 4,679 breaches of Part 9, making it the Code Part with the second highest breaches in this reporting period.

Table 11: Breakdown of Part 9 Code breaches, By Chapter

Chapter	Jan-Jun 2021	Jul-Dec 2021	% change
39 Contact us if you are experiencing financial difficulty	712	1,708	↑ 140%
40 We may contact you if you are experiencing financial difficulty	19	21	↑ 11%
41 We will try to help you if you are experiencing financial difficulty	1,142	861	↓ 25%
42 When you are in default	68	149	↑ 119%
43 When we are recovering a debt	1,915	1,662	↓ 13%
44 Combining your accounts	5	1	↓ 80%
45 Helping with deceased estates	291	277	↓ 5%
Total	**4,152**	**4,679**	**↑ 13%**

The major banks collectively accounted for 97% of Part 9 breaches. Three of the major banks reported an increase in the Part 9 breaches in the current and previous reporting period. In contrast, Major Bank 2 reported a decrease in both periods. Major Bank 2 attributed the decrease to system and technology enhancements and continued focused staff development, which goes to our recommendation that, while better trained staff reduce errors, improved systems, processes and controls are key to decrease the risk of Code breaches and other errors.

In this reporting period, Major Bank 3 reported a 126% increase of Part 9 breaches and accounted for 50% of the total breaches reported under Part 9. 57% of its Part 9 breaches are of Chapter 39. Most of its Chapter 39 breaches related to delay in responding to the customer's hardship request. Major Bank 3 explained that a continued high volume of hardship requests and with the hardship process requiring a high amount of manual inputs, made it hard to adhere to the Code timeframes.

Banks sample

Banks provided further information on 287 incidents, constituting 2,537 breaches and impacting more than 79,000 customers.

Banks reported 67% of the incidents were the result of human error and were corrected through staff training, coaching or feedback. While human error remains the predominant cause of the breaches, the banks' sample shows system errors and deficiencies in processes/procedures resulted in the highest customer impact. Banks identified:

- system errors which impacted approximately 6,965 customers
- deficiencies in processes and procedure which impacted approximately 58,423 customers.

Part 10 – Resolving your complaint

Part 10 of the Code (Chapters 46 – 49) contains requirements for how banks should communicate with customers when resolving complaints. It also contains the Code obligations for the establishment of the BCCC.

Banks reported 2,181 breaches of Part 10 for this period. This is a 52% increase compared with the 12% decrease reported in the last reporting period.

Table 12: Breakdown of Part 10 Code breaches, By Chapter

Chapter	Jan-Jun 2021	Jul-Dec 2021	% change
46 Our Customer Advocate	0	0	-
47 If you have a complaint about us	658	318	↓ 52%
48 How we handle your complaint	776	1,862	↑ 140%
49 Code monitoring, complaints and sanctions	0	1	↑ 100%
Total	**1,434**	**2,181**	**↑ 52%**

Banks attributed the increase to the introduction of the ASIC Regulatory Guide 271: Internal Dispute Resolution (RG 271) which came into effect on 5 October 2021. RG 271 updated the requirements on how financial firms should deal with complaints under their Internal Dispute Resolution (IDR) procedure. It requires financial firms to record all complaints received and have an effective system for recording information about complaints.

Major Bank 2, Major Bank 3 and Bank A which collectively accounted for 83% of the breaches, have explained that they have implemented a new complaints management system and introduced process changes that improved their capability in identifying more breaches. These changes, along with the increased focus on complaints management, have resulted in the overall increase in Part 10 breaches.

Banks' sample

Banks provided further information on 169 incidents, constituting 575 breaches and impacting more than 7,000 customers.

While banks reported 92% of the incidents were caused by human error, a significantly larger number of customers were impacted due to deficiencies in processes and procedures. The sample shows approximately 68% of customers were impacted due to deficiencies in processes and procedures.

Appendix 1: About the BCCC and the Compliance Statement

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:

- examines banks' practices
- identifies current and emerging industry wide problems
- recommends improvements to bank practices
- sanctions banks for serious compliance failures
- consults 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.

The following represent the priority areas that we are focusing on in 2022–23:

- follow up on the Guarantees Inquiry Report
- deceased estates
- issues impacting Small Business and Agri-business customers
- follow up on 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 its Code Monitoring Priority Framework.

Further information about us and members of the Committee is available on our website.

Banking Code Compliance Statement

We developed the Banking Code Compliance Statement (Compliance Statement) to collect breach data from banks. The Compliance Statement program is conducted in accordance with clause 4.2 of our Charter.

It enables us to:

- benchmark banks' 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 further details where breaches met 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 had an impact on 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 were required to report details for a random sample of 5% of the remaining breaches of each Code Chapter.

We require banks to report breaches at an incident level. Banks were required to describe an incident, event or action and then list one or more Code obligations that had been breached as a result.

'Three lines of defence'

For this report, we have referred to the three lines of defence. This model is commonly used by subscribing banks and refers to the three "lines" within a business unit responsible for addressing compliance risk. While the model is applied in different ways by banks, 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
- second line – the specialist function that develops risk management policies, systems and processes
- third line – internal audit with responsibility for reviewing the effectiveness of the compliance framework and independently reporting to the Board.[8]

[8] More detail about the three lines of defence risk governance model can be found here: Australian Prudential Regulation Authority, *Prudential Practice Guide – CPG220 Risk Management*, April 2018.

BCCC Contact Details

Website:	bankingcode.org.au
Email:	info@codecompliance.org.au
Media enquiries:	media@codecompliance.org.au
Postal address:	PO BOX 14240 Melbourne VIC 3001

BCCC
Banking Code
Compliance Committee