BCCC
Banking Code
Compliance Committee

Banks' compliance with the Banking Code of Practice

July to December 2019

August 2020

Contents

Message from the Independent Chair

As the Independent Chair of the Banking Code Compliance Committee (BCCC), I am pleased to present this report on Code subscribing banks' (banks) compliance with the Banking Code of Practice (Code).

The BCCC requires banks to self-report on their compliance with the Code every six months. This report provides a high-level summary of banks' compliance with the Code for the period July to December 2019. The BCCC will publish a report on banks compliance for the full 2019–20 reporting period in early 2021.

What are banks self-reporting?

Banks reported 20,863 Code breaches for the six-month period. These breaches affected at least 4.4 million customers and had a financial impact of more than $100 million.

Data at a glance

20,863 **Breaches of the Code**

4.4 million **Customers affected by breaches**

$100 million **Financial impact of breaches**

Privacy and confidentiality remains the most commonly breached Code obligation. In a change to previous reporting, the second highest category of Code breaches is now Chapter 4 which includes banks' obligations to train staff to understand the Code and engage with customers in a fair, reasonable and ethical manner.

Table 1. Top 6 Code Chapters breached

Code Chapter	Number of breaches
05 Protecting confidentiality	5,869
04 Trained and competent staff	4,726
17 A responsible approach to lending	2,446
43 When we are recovering a debt	1,703
39 Contact us if you are experiencing financial difficulty	1,567
48 How we handle your complaint	1,171

Banks' reporting about how they remediate customers continued to improve since previous periods. They provided remediation details for approximately 97% of Code compliance incidents.

An increase in breaches

For the 2018–19 12-month period, banks reported 15,597 breaches. The 20,863 breaches identified between July and December 2019 represents a significant increase in reporting. This increase raises complex questions for the BCCC - does the increase mean that some banks are finally taking on board previous feedback about under-reporting Code breaches? Or is the increase a cause for concern – is there a growing trend of more customers not receiving the full protection that the Code provides?

The Committee has long held a view that some banks continuously under-report on their compliance with the Code. We are still unable to conclude definitively whether the increase in breaches reported each year represents a deterioration in bank conduct, or is a demonstration that banks are better able to identify and fix problems. The Committee considers that the latter explanation remains the more likely explanation.

In our Report on Banks Transition to the 2019 Code, published in November 2019, the BCCC noted:

> *Banks' compliance frameworks may not currently be mature enough to comprehensively monitor Code compliance from 1 July 2019 to the BCCC's satisfaction. Banks' responses often indicated that they would be continuing to amend their controls and compliance frameworks post 1 July 2019, particularly for small business, vulnerability and financial difficulty obligations.*
>
> *This raises a concern that non-compliance may go undetected in the interim and remain that way until banks have improved their Code monitoring controls.*

With this increase in breaches, the BCCC is encouraged that some banks are making progress. Banks often explained that the increases in reporting were the result of efforts to increase awareness and monitoring of Code compliance, and improve risk culture.

Nevertheless, it is worth noting that the overall increase in breaches for this period is due to significant increases reported by just two banks, which account for 72% of the total number of breaches.

These banks have explained that their revised approach to reporting is largely in response to guidance and feedback provided by the BCCC. The BCCC requires

banks to consider all Code obligations when conducting any compliance assessments and not just those that are aligned to existing legislation or regulation. In addition, while we recognise that banks may report legislative or regulatory breaches to regulators based on an assessment of a breach's significance or materiality, the Code and BCCC Charter make no reference to such thresholds - banks are required to record all Code breaches.[1]

We strongly encourage all banks to make sure they are taking this approach and ensure compliance frameworks enable them to identify, record and report Code breaches.

Data quality concerns

While the quality of data reported is generally better than we have received previously, there remains substantial room for improvement. Now, more than ever, it is important that banks' data is of a high standard because banks are reporting data every six months. High quality responses reduce the need for the BCCC to seek clarification about data from banks or ask banks to address any data gaps.

Some banks appear to be copying data directly from internal systems without proper curation or regard for reporting requirements. We recognise the BCCC's reporting requirements are extensive, but the data provided must sufficiently explain what has occurred, and the steps taken to remediate customers and prevent recurrence.

Thorough and accurate breach reporting is a demonstration of a customer-focused culture and a bank's commitment to embedding the Code. We will pay close attention to whether banks are taking their obligations seriously and we strongly encourage banks to ensure that sufficient resources and time are applied to the BCCC's reporting requirements.

We have provided banks with additional time to respond to the next Compliance Statement, to ensure banks can focus on supporting customers during the COVID-19 pandemic. In addition, we have reduced the scope of the information we will request under the next Compliance Statement.

The BCCC will provide individual feedback about data quality issues to relevant banks. Banks should ensure the issues are addressed for future reporting.

Ian Govey AM
Independent Chairperson
Banking Code Compliance Committee

[1] Guidance Note No. 1: Breach Identification and Reporting, September 2019
Guidance Note No. 2: Clause 10 – fair, reasonable and ethical behavior, November 2019

About the Code, the BCCC and the Report

The Code

The Code sets out the standards of practice and service in the Australian banking industry for individual and small business customers, and their guarantors.

19 banks subscribe to the Code.

The BCCC

The BCCC is an independent compliance monitoring body established under clause 207 of the 2019 Code. The purpose of the BCCC is to monitor and drive best practice Code compliance.

One of the primary ways the BCCC monitors banks' compliance with the Code is through the Banking Code Compliance Statement.

The Banking Code Compliance Statement

The BCCC 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 the BCCC Charter. It enables the BCCC to:

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

What's new about the Compliance Statement

Banks are now reporting breach data twice a year

Banks reported breaches of the 2019 version of the Code for the first time

Six new Code subscribers reported breach data to the BCCC for the first time

Banks are required to provide breach data twice a year for the preceding six-month reporting period.

Banks were required to report the total number of breaches they identified during the reporting period.

Banks were also required to provide 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 clause. For previous reporting periods banks reported which obligation had been breached and then described what occurred.

This time and moving forward banks are required 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.

The Report

This report summarises banks' Code breach data for the reporting period of July to December 2019.

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". Banks are not labelled consistently throughout, meaning Bank A in one section may not be labelled Bank A in another section.

The BCCC has classified and reported on the breach data by reference to which 'Part' of the Code the incident or breach most clearly aligned with and includes a more detailed examination of specific chapters and sections where necessary.

Banks provide data about the overall number of breaches, and then further details for a significant sample of these.

As a result, the number of breaches 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 below.

The BCCC has also included de-identified examples based of individual breaches where the incident is of particular interest or concern.

As this report covers a six-month period, it contains Code provisions that were not in the 2013 version of the Code and includes data for six new subscribers, which created challenges to providing meaningful comparisons with data from previous reporting periods.

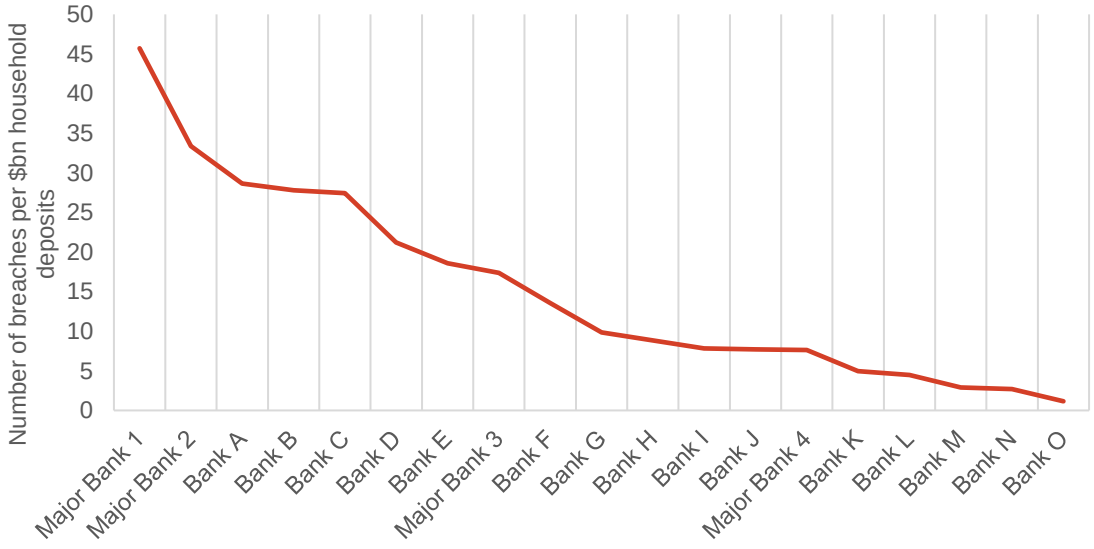
The BCCC anticipates that further comparison of trends will be undertaken after banks provide data for the full 2019-20 reporting period in the next Compliance Statement.

Summary of breaches overall

Banks reported 20,863 breaches of the Code for the period July – December 2019.[2]

For benchmarking purposes, Chart 1 displays comparative figures based on the size of the bank using the Australian Prudential Regulation Authority's December 2019 monthly banking statistics for household deposits.[3] The industry average is 23 breaches per $1billion of household deposits.

Chart 1. Number of breaches per $bn household deposits, by bank



The Code is made up of ten 'Parts'. Each Part of the Code is made up of Chapters which detail obligations about service standards for specific aspects of a customer's banking experience or for a specific type of customer.

More than 50% of all the reported breaches fall under Part 2 of the Code. Part 2 includes obligations to protect a customer's privacy and confidentiality, train staff to understand the Code and engage customers in a fair, reasonable and ethical manner.

Table 2 provides a breakdown of breaches by the various 'Parts' of the Code.

[2] Banks reported breaches under the framework of the 2019 Banking Code, but the data includes breaches of the 2013 version of the Code.

[3] https://www.apra.gov.au/news-and-publications/apra-releases-monthly-authorised-deposit-taking-institution-statistics-for-1. The BCCC has calculated the figures by dividing the total number of breaches reported by each bank by the APRA figure for total household deposits held by the bank in December 2019.

Table 2. Number of breaches, by Code section

Code section	Number of breaches	Percentage of total
Part 2 Your banking relationship	10,957	53%
Part 9 When things go wrong	3,949	19%
Part 5 When you apply for a loan	2,456	12%
Part 3 Opening an account and using our banking services	1,461	7%
Part 10 Resolving your complaint	1,248	6%
Part 8 Managing your account	447	2%
Part 4 Inclusive and accessible banking	154	<1%
Part 7 Guaranteeing a loan	107	<1%
Part 6 Lending to small business	68	<1%
Part 1 How the Code works	15	<1%
Transition Period	1	<1%
Total	**20,863**	

Approach to analysis

In accordance with the BCCC's instructions (see p. 7), banks provided further information about the nature, cause, impact and correction of 2,411 incidents, constituting 10,387 breaches – 50% of the total reported. The rest of this section of the report refers only to this subset of incidents.

What caused the breaches

Banks reported that the majority of incidents (60%) were caused by human error alone, 13% involved a control, training or resourcing failure (including process deficiencies) and 13% involved a system error. Banks reported that 8% of incidents were caused by human error along with another cause.

This is a significant and welcome change to previous reporting. For the last two years banks reported that over 90% of breaches were caused by human error and the BCCC was concerned that banks were attributing breaches to human error without conducting a thorough root cause analysis. While the BCCC cannot determine with certainty that this change is due to more in-depth analysis by banks, it seems unlikely that the nature of the breaches would have changed in such a considerable way over the last 12 months. The BCCC encourages banks to continue to look beyond human error alone and identify underlying causes, including those related to systems, processes, training and culture.

The BCCC will shortly publish the findings of research it commissioned about how banks can build organisational capability – through systems, culture and staff training – to support Code compliance.

How the breaches were identified

For this report, the BCCC has where appropriate referred to the three lines of defence framework. This framework 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, and
- third line – internal audit with responsibility for reviewing the effectiveness of the compliance framework and independently reporting to the Board.[4]

The Compliance Statement is based on banks' ability to self-identify Code breaches. It is crucial to the BCCC's work to understand how banks are identifying whether Code breaches have occurred.

30% of incidents were self-identified by staff members. The other most prominent methods of breach identification were via a customer complaint, query or feedback (27%), and line 1 quality assurance activities including call monitoring (23%). A further 9% of incidents were identified by line 2 or internal reviews.

The BCCC is encouraged that the most common method of breach identification is by staff themselves identifying Code breaches in the first instance. This may indicate that employees' awareness of Code provisions and compliance responsibilities is increasing.

The impact of the breaches

Banks reported 2,411 incidents that caused 10,387 breaches. The breaches impacted more than 4.4 million customers, with a total financial impact of over $100 million.

Table 3. Impact of Code breaches, by bank

Bank	No. of incidents reported	Customers impacted	Financial impact ($)
Major Bank 1	688	920,589	29,202,228
Major Bank 2	458	1,232,197	39,419,111
Major Bank 3	382	1,414,544	21,954,540
Major Bank 4	183	318,551	5,214,999
Bank A	170	6,888	1,676,703
Bank B	125	2,537	80,990
Bank C	82	63,725	737,868

[4] More details about this the three lines of defense risk governance model can be found here: Australian Prudential Regulation Authority, *Prudential Practice Guide – CPG220 Risk Management* (2018)

Bank D	82	131,493	210,395
Bank E	78	11,837	365,135
Bank F	37	278,741	1,497,512
Bank G	27	3,902	1
Bank H	24	15,672	7,445
Bank I	20	27,710	12,224
Bank J	17	33,176	72,295
Bank K	16	2,911	-
Bank L	12	19,922	-
Bank M	7	10	3,337
Bank N	2	2	-
Bank O	1	1	-
Total	**2,411**	**4,484,408**	**100,454,783**

How the breaches were corrected

The BCCC collects data about how banks both prevent the recurrence of breaches and take steps 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:

- provide staff training, coaching or feedback (59% of incidents)
- review and/or improve processes (12%)
- implemented a system fix (9%)
- enhance monitoring or controls (4%), and
- review staff performance or taken disciplinary action (5%).

Bank actions to prevent recurrence were still under review at the time of reporting for 9% of incidents. Banks did not provide details of efforts to prevent recurrence for 5% of incidents. Banks reported that they did not take actions to prevent recurrence or no action was required for 2% of incidents.[5]

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

- corrected the individual issue, including updating details, and requests for information be destroyed, deleted or returned (30% of incidents)
- refund, compensation or goodwill payment provided (18%)
- communicated or corresponded with the customer (12%)

[5] Data may not total 100% because banks may have taken **one or more** of the actions listed.

- apologised to the customer (7%)
- logged, managed or resolved a complaint (3%)
- customers referred for financial difficulty assistance (<1%), and
- a reduction in liability, repayment arrangement or collection activities put on hold or ceased (<1%).

Banks reported there was no customer remediation provided or customer remediation was not required for 20% of incidents. For 11% of incidents, the breach incidents were still under investigation at the time of reporting and banks had yet to complete customer remediation.

Banks did not provide details of remediation activities for 3% of incidents or confirm that these breaches were still under investigation. The BCCC will follow up the banks involved to ensure that complete information is provided in the future.

Part 2 – Your banking relationship

Part 2 of the Code, 'Your banking relationship,' includes Chapters 3 to 7. Banks reported the highest number of breaches for this part of the Code - 10,957. Two banks accounted for 78% of the breaches reported under Part 2.

Table 4. Number of breaches reported under Part 2 of the Code, by Chapter

Code Chapter	Number of breaches
03 Our compliance with this Code	333
04 Trained and competent staff	4,726
05 Protecting confidentiality	5,869
06 Compliance with laws	28
07 Closing a branch	1
Total	**10,957**

Chapter 3 requires banks to 'comply with the Code.' The BCCC does not expect banks to report breaches under Chapter 3 because a breach of any Code obligation will also be a breach of Chapter 3.[6]

The rest of this section of the report focuses on Chapter 4 and Chapter 5.

Chapter 4 – Trained and competent staff

It is too complex to make a direct comparison with other reporting periods for Chapter 4 breaches. 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. These obligations were included under different sections of the 2013 Code.

Further, the new approach to breach reporting means that the BCCC expects banks to consider multiple categories of breaches for each incident. For example, an incident which led to a breach of financial difficulty obligations might also be a breach of the requirement to treat customers fairly and reasonably.

Banks reported a total of 4,726 breaches of Chapter 4. One major bank reported 70% of the breaches of Chapter 4. The bank that reported most of the incidents under Chapter 4 noted in its submission that the majority of breaches were where the bank had failed to act fairly and reasonably towards customers. Three banks did not report any breaches of Chapter 4.

Nevertheless, it appears there has been a significant increase in reporting breaches of these obligations, in particular for fair and reasonable conduct. Banks reported a combined 745 breaches of almost equivalent provisions in the 2013 Code for 2018-19.

[6] See p. 3, Guidance Note No. 1: Breach Identification and Reporting, September 2019

In accordance with the BCCC's reporting criteria (see p.7), banks provided further information about the nature, cause, impact and correction of 567 incidents under Chapter 4.

Nature of incidents

The nature of the incidents reported under Chapter 4 varied greatly, largely because of the broad obligation for the bank and its staff members to engage with customers in a fair, reasonable and ethical manner.

Examples of incidents reported under Chapter 4 by banks include:

- Processes not followed correctly
- Fees incorrectly charged
- Information provided or disclosed to an incorrect party
- Delays in directing complaints to the appropriate complaints handling team
- Incorrect correspondence provided to customer
- Incomplete or inaccurate file notes
- Interest or discount errors
- Terms and conditions containing incorrect or missing information
- Identification errors
- Not complying with Terms and Conditions

What caused the incidents

Banks reported that human error was the cause of most incidents under Chapter 4 (40%). The second highest cause of breaches was reported as being a system error, system failure or system issue (17%). The third highest was control, training or resourcing error (17%).

How the incidents were identified

Banks reported that incidents under Chapter 4 were most commonly self-identified or reported by bank staff members (27%) or identified through line 1 monitoring and quality assurance (29%), customer complaints (22%) and internal reviews (13%).

The impact of the incidents

The financial impact of the Chapter 4 incidents was significant. 1,814,404 customers were affected, with a total financial impact of $57,280,979 – more than half the total impact of all breaches.

How the breaches were corrected

The most common step taken by banks to prevent recurrence was, as one might expect for this chapter of the Code, staff training, coaching or feedback. The second most likely corrective action was a system fix.

For 31% of incidents, banks did not remediate the customer or found that customer remediation was not required. The most common remedial action was to refund or reimburse

customers (23%), followed by the correction of the individual issue the incident related to (13%).

For 12% of breaches of Chapter 4, banks had yet to remediate the customer or were continuing to investigate the issue.

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 5,869 breaches reported for this period.

Banks provided further information about 665 incidents including their nature, cause, impact and correction. The rest of this section of the report refers only to this subset of breaches.

Nature of the incidents

Where banks provided further detail, the breaches were of a similar nature to those reported in previous compliance statements.

One major bank reported an incident that accounted for 1,777 breaches. No other individual privacy breach counted for as many breaches. The incident related to the bank's internal policy about redacting credit card numbers.

The second highest category for a type of incident was when information was provided or disclosed to the incorrect party. This type of breach includes, for example, when a bank sends correspondence to an incorrect address, or verbally provides information to the incorrect customer. Further, it includes when a bank staff member inadvertently emails correspondence to the incorrect address, or when a bank staff member misplaces confidential documents or information. In the past, this type of incident has had the highest number of breaches.

What caused the incidents

Banks overwhelmingly reported that incidents were caused by human error (78%), or human error plus some other cause (9%). This is not unexpected as many breaches are likely to be the result of an inadvertent or accidental error by staff members. Nevertheless, the BCCC encourages banks to review the root cause(s) of such incidents and develop controls that limit the likelihood of human error. A system error, failure or issue was cited as the cause of 6% of incidents, and a control, training or resourcing error was cited as the cause for 3% of incidents.

How the incidents were identified

Banks reported that most incidents were self-identified or reported by a bank staff member (36%). The second highest reported method of identification was customer complaints (30%). The BCCC is encouraged that staff awareness of their privacy and confidentiality obligations supports the self-identification of breaches.

The impact of the incidents

The privacy and confidentiality breaches impacted 1,180,697 customers, with a financial impact of $1,603,422.

How the breaches were corrected

Banks overwhelmingly corrected incidents with further staff training, coaching or feedback (58%). Other actions to prevent recurrence included:

- system fix (13%)
- process reviews and/or improvements (9%)
- enhanced monitoring or controls (3%)

The primary way that most incidents were remediated was with the individual issue being corrected (35%), and this often involved a request for information to be destroyed, deleted or returned (11%). The second most common way that incidents were remediated was by way of customer apology (10%). For 13% of incidents, banks reported there was no customer remediation, or remediation was not required.

Part 3 – Opening an account and using banking services

Part 3 of the Code contains Chapters 8 to 12, which 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 1,461 breaches of Part 3 obligations and further details about 347 incidents.

The nature and impact of the incidents

Part 3 incidents mostly related to non-disclosure or incorrect disclosure of required information to customers. This included incorrect correspondence being sent to customers, statements not being provided in accordance with terms and conditions or call centre staff not reading all the required scripted information.

Other breaches were for a variety of incidents, such as non-disclosure of break fees, incorrect interest rates being charged, and a variety of system or process errors resulting in customers not receiving responses to requests within required timeframes.

The total financial impact reported was approximately $5,117,000, with 822,473 customers affected.

What caused the incidents and how they were identified

Banks reported that most of the incidents (51%) were caused by human error and 22% of incidents were caused by control or training issues.

Banks reported that breaches of Part 3 obligations were identified by methods including:

- customer complaints (29% of incidents)
- line 1 monitoring and quality assurance (17%)
- staff self-reporting (31%)
- internal reviews (12%)

How the breaches were corrected

Banks generally remediated customers by correcting individual issues (22%), providing refunds (14%) and/or apologising to customers (6%). Banks reported that for 19% of incidents no remediation was required.

For 37% of incidents, banks reported that they provided staff with additional training to prevent recurrence. 38% required system and/or process fixes, 13% of incidents were still under investigation and the remainder were either not required or no information was provided.

Part 4 – Inclusive and accessible banking

Banks reported 154 breaches of Part 4 of the Code. Part 4 of the Code includes the obligations banks owe to customers experiencing vulnerability, Indigenous customers and people with a low income.

Seven banks did not report any breaches of obligations under Part 4. The BCCC understands that many of the obligations under Part 4 are new requirements and in some cases, banks may be continuing to develop policies, processes and staff training to meet these requirements.

Nevertheless, the BCCC encourages banks to make every effort to identify breaches of these obligations. The BCCC has commenced an Inquiry into these obligations and the Inquiry will further explore banks efforts to monitor compliance with Part 4 of the Code.

Table 5. Number of breaches reported under Part 4 of the Code, by Chapter

Code Chapter	Number of Breaches
13 Being inclusive and accessible	25
14 Taking extra care with customers who may be vulnerable	101
15 Banking services for people with a low income	18
16 Basic accounts or low or no fee accounts	10
Total	**154**

Banks provided further information about the nature, cause, impact and correction of 32 incidents related to Part 4. The rest of this chapter refers only to this subset of incidents and associated breaches.

Nature of the incidents

The nature of the incidents banks reported can be broadly categorised as bank staff:

- not taking appropriate care with customers experiencing vulnerable circumstances or not considering a customer's vulnerability when providing a service
- failing to ask customers if they hold a concession card
- not offering low or no fee accounts to low income earning customers, and
- suggesting to customers living remotely to visit a branch to solve their issue.

Other issues included accessibility issues with an iOS application and a failure to restrict withdrawals from a customer's account when required.

Cause and identification of the incidents

Banks reported that most of the incidents (53%) were the result of human error. A further 16% were the result of human error, plus another cause. 19% were the result of a control, training or resourcing error.

Banks identified Part 4 incidents following complaints from the customer in 65% of cases, followed by line 1 monitoring activities (12%).

The impact of the incidents

11,978 customers were impacted by the incidents reported under Part 4 of the Code, with a financial impact of $1,268,248.

9,900 customers (with a financial impact of $720,891) were affected by a single breach reported by one major bank where the bank closed credit card accounts with a credit balance. The incident was still under investigation at the time of reporting.

How the breaches were corrected

Banks corrected breaches predominantly through staff training, coaching or feedback (59%).

Banks' remediation included:

- customer refunds or reimbursement (28%)
- individual issue corrected (19%)
- apologising to the customer (16%)
- monitoring customers' accounts (3%)

Part 5 – When you apply for a loan

Banks reported 2,456 breaches of Part 5 of the Code.

Part 5 includes Chapter 17 to 19, which contain the provisions relating to responsible lending. Most of the breaches reported under Part 5 were in relation to responsible lending. Chapter 17 requires banks to exercise the care and skill of a diligent and prudent banker when considering providing a new loan, or an increase in a loan limit, to both individual and small business customers.

Chapter 18 outlines banks' requirements for selling consumer credit insurance (CCI). Banks reported 10 breaches of Chapter 18. Chapter 19 sets out the requirements for lender's mortgage insurance. No bank reported a breach of Chapter 19.

The following section of the report will focus on breaches of Chapter 17 of the Code - *a responsible approach to lending*.

Incident trends

Banks reported a total of 2,446 breaches of Chapter 17. As discussed earlier, there are limitations to comparing the data to previous reporting periods, given that there are six new subscribing banks and the data is only for a six-month period. Nevertheless, this is broadly comparable with the number of breaches reported for 2018-19 when banks reported 4,066 breaches for the 12-month period.

Consistent with previous years, one outlier bank reported most of the breaches (58%). Eight banks did not report any breaches of Chapter 17. For three of the existing Code subscribing banks, this was the second consecutive Compliance Statement where it reported no responsible lending breaches.

Banks provided further information about the nature, cause, impact and correction of 300 responsible lending incidents. The rest of this section refers only to this subset of incidents.

Nature of the incidents

Most of the Chapter 17 breaches were the result of an irresponsible or incorrect lending decision. For some breaches, banks reported that they did not make sufficient enquiries about a customer's needs or financial situation, or the bank made an incorrect assessment of customer's situation.

What caused the incidents

Banks considered that the responsible lending breaches were overwhelmingly the result of human error (63% of incidents). Approximately 5% of incidents were the result of human error and another cause. 14% of incidents were the result of a control, training or resourcing error and 7% the result of a system issue.

For 10% of incidents, banks reported that there was an ongoing investigation to understand the cause, or the bank had not given a sufficient response to understand the cause.

How the incidents were identified

The responsible lending incidents were identified by methods including:

- line 1 monitoring activities (33% of incidents)
- a complaint (made directly or via AFCA) (34%)
- self-identification by a staff member (22%)
- line 2 / internal reviews (7%)

The impact of the incidents

The financial impact of the responsible lending incidents amounted to $8,988,547, with 13,168 customers affected.

How the breaches were corrected

Banks reported actions to prevent recurrence of breaches which most often included, providing staff training, coaching and feedback (54% of incidents).

For 12% of incidents, banks reported that there was an ongoing investigation into the incident, and no corrective action had been undertaken. For 11% banks provided no information as to the corrective action undertaken and for 2% banks reported that no corrective action was required.

Where banks provided further information, banks remediated the customer by:

- providing a refund or reimbursement to the customer (19% of incidents)
- correcting the individual issue (9%)
- communicating with the customer (5%)
- a liability reduction, repayment arrangement or ceased collections activity (4%)
- providing compensation (3%)
- dealing with a customer's complaint (2%)

For 17% of incidents, banks reported that there was an ongoing investigation into the matter or customer remediation was not yet completed. Banks reported that there was no customer remediation provided or customer remediation was not required for 30% of incidents. For 8% of incidents, banks did not provide information about customer remediation.

Part 6 – Lending to small business

Part 6 of the Code contains obligations about lending to small business customers.

Banks reported 68 breaches under Part 6 of the Code. Only five banks reported breaches of the obligations under Part 6.

Table 6. Number of breaches reported under Part 6 of the Code, by Chapter

Code Chapter	Number of Breaches
20 Helping a small business when it applies for a loan	59
21 When will we not enforce a loan against a small business?	1
22 Specific events of non-monetary defaults	0
23 When we decide not to extend a loan	2
24 When we appoint property valuers, investigative accountants and insolvency practitioners	6
Total	**68**

The nature and impact of the breaches

The majority of the breaches (76%) were reported by a major bank and involved staff members failing to provide a pre-application notification to small business customers in accordance with the requirements of Chapter 20.

One breach by another bank was caused by the bank repossessing equipment before the expiry date on a notice of demand. This breach had a reported financial impact of $1,056 which was refunded to the customer.

The breaches were reported to have affected 150 customers in total.

What caused the breaches and how they were identified

The majority of incidents were caused by human error apart from one, which was caused by a process design issue/control, training or resourcing error.

Most of the breaches were identified by Line 1 monitoring activities.

How the breaches were corrected

For most of the breaches banks provided staff training and feedback, and small business customers were provided with the relevant information.

Part 7 – Guaranteeing a loan

Part 7 of the Code contains the obligations for guaranteeing a loan and are some of the most prescriptive requirements within the Code. Chapters 25 to 29 include detailed requirements such as a guarantor's right to limit or end a guarantee, and banks' obligations to provide notices (for example that the guarantor should seek independent legal and financial advice), and any adverse credit information about the borrower's financial position.

Banks are required to provide prospective guarantors with extensive information prior to entering into a guarantee, and there are strict conditions around the signing of a guarantee.

Guarantees remain a priority focus area for the BCCC and a major Inquiry into the obligations is in progress.

Banks reported 107 breaches of guarantee provisions. Two major banks accounted for 64% of these breaches. The eight other banks that reported guarantees breaches each reported fewer than ten breaches.

Banks provided further information about 44 incidents that led to breaches of Part 7.

The nature of the incidents

A significant proportion of the incidents reported relate to the non-disclosure of required information to the guarantor.

There were a small number of incidents across the banks where the signing provisions of the Code had not been adhered to. These included borrowers and guarantors being allowed to sign together, and in one case bank staff were present to witness the guarantor's signature.

One incident reported by a bank led to serious concerns about the enforceability and validity of the guarantee. These concerns were such that the bank has flagged the loan in case it falls into arrears and for the bank's legal team to be consulted prior to any enforcement action.

Other notable breaches are referred to in the impact section below.

The impact of the incidents

The 44 incidents affected 486 customers, with a total financial impact of $1,120,810.

One bank reported a breach that affected 74 customers (guarantors) where they had not been provided all of the required guarantee disclosure documents.

One major bank reported a breach that affected 193 customers where loans had fallen into default and guarantors were not provided with the required default notice and financial difficulty assistance outcome letters. This bank also reported a similar breach affecting another 11 customers.

Another major bank reported a breach of a similar nature affecting 104 customers.

As noted above, the majority of breaches reported under Part 7 related to failure to or late to provide required disclosures and documents and in these cases no financial impact was recorded.

One major bank reported five breaches which constituted all of the total financial impact recorded. Two of these breaches involved guarantors being given incorrect information and the bank providing $10,000 to each guarantor in the form of settlements.

The other three relevant breaches were a result of AFCA determinations that found the guarantees were unenforceable. Further details are provided below.

- AFCA found that the bank breached its obligations to the complainant when it provided the guarantee and indemnity documents for signing to the broker, who was representing the complainant's former partner. The bank did not give a copy of the loan and guarantee and indemnity documents to the complainant who was also a guarantor. Financial impact on the bank $427,005.
- AFCA found that the bank had not been able to demonstrate it complied with the guarantee provisions of the Code when it provided the guarantee documents to the complainant for signing. As such, the guarantee and supporting mortgage provided by the complainant were considered unenforceable. Financial impact on the bank $452,805.
- AFCA found that the bank did not comply with its obligations in obtaining the guarantee because it could not demonstrate it met with the complainant to discuss the loan application, or that the loan documentation was issued to the complainant. The bank could also not demonstrate that the complainant had the appropriate time of 24 hours to consider the guarantee before signing it. Financial impact on the bank $220,000.

What caused the incidents and how they were identified

Banks reported human error as the cause of 64% of incidents. 16% of incidents were the result of a system error, failure or issue.

52% of incidents were identified by Line 1 monitoring activities.

How the breaches were corrected

The most common action taken to prevent recurrence was staff training and coaching (for 62% of incidents).

Information provided by banks about customer remediation was often unclear. In some cases, banks described providing information to the customer (guarantor) generally or described actions in such a way that did not confirm the action had been completed. The BCCC reminds banks that when reporting information about customer remediation there should be a clear description about the steps that have been taken to rectify the issue.

Part 8 – Managing your account

Part 8 of the Code includes Chapters 30 to 38 which largely cover obligations about day to day transactional banking services.

Banks reported 447 breaches of Part 8 of the Code.

Four banks did not report any breaches of obligations under Part 8. It was surprising that banks reported zero breaches of Part 8 of the Code, given that Part 8 includes nine chapters and contains a high number of obligations on banks.

The highest number of reported breaches under Part 8 was for Chapter 34, which includes the obligation for banks to cancel a customer's direct debit on request. This is not unexpected as the BCCC has ongoing concerns about banks' ability to comply with the direct debit obligations under the Code.

Table 7. Number of breaches reported under Part 8 of the Code, by Chapter

Code Chapter	Number of breaches
30 Keeping your accounts safe and secure	10
31 Statements we will send you	16
32 Cost of transaction service fees	18
33 Managing a credit card	62
34 Direct debits and recurring payments	147
35 Joint Accounts	32
36 Closing any of your banking services	114
37 Your right to copies of certain documents	13
38 When we change our arrangements with you	35
Total	**447**

Banks provided further information for 110 incidents that led to Part 8 breaches.

Nature of the incidents

Banks reported a wide range of incidents as breaches under Part 8. Some examples include:

- Banks not following a customer's instructions (for example, not actioning a customer's request correctly, not following a customer's request to close their account or not following a customer's request to cancel a direct debit).
- Banks not following processes correctly (for example, chargeback requests processed incorrectly, customer accounts closed without reasonable notice and transaction dispute processes not followed).

- Banks provided customers with incorrect information about direct debits, joint account authority, fees and charges, and interest rates.
- Banks failing to provide customers with requested information.
- Statement errors (for example, statements not sent or delayed or sent to a wrong address).

What caused the incidents

Banks reported 61% of breaches were caused by human error. For 5% of incidents, the cause was human error in conjunction with another cause

Other causes of incidents included a:

- control, training or resourcing error (15%)
- system error, failure or issue (15%)

For 22 breaches (<1% of incidents), banks did not report the cause and for 2% of incidents, banks reported that there was an ongoing investigation into the cause, or banks provided an insufficient response to understand the cause.

How the incidents were identified

Banks identified breaches of Part 8 obligation by methods including:

- customer complaint, query or feedback (45% of incidents)
- staff members self-identifying or self-reporting breaches (20%)
- line 1 monitoring, quality assurance or call monitoring (17%)
- line 2 or internal review (4%)

The impact of the incidents

The number of customers impacted by Chapter 8 incidents was 357,624, with a financial impact of $535,775.

How the breaches were corrected

The main corrective action taken by banks was staff training, coaching and feedback.

Banks primarily remediated customers by correcting the individual issue (23% of incidents). For 16% of incidents, banks reported that customers were remediated by way of customer refund or reimbursement.

For 15% of incidents, banks reported that there was an ongoing investigation into the incident, or that customer remediation had yet to commence. For 11% of incidents, banks reported that there was no customer remediation or customer remediation was not required. For another 11% of incidents, banks did not provide enough information to deduce what customer remediation was undertaken.

Part 9 – When things go wrong

Part 9 of the Code 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 3,949 breaches of Part 9 of the Code.

Table 8. Number of breaches reported under Part 9 of the Code, by Chapter

Code Chapter	Number of breaches
39 Contact us if you are experiencing financial difficulty	1,567
40 We may contact you if you are experiencing financial difficulty	123
41 We will try to help you if you are experiencing financial difficulty	327
42 When you are in default	6
43 When we are recovering a debt	1,703
44 Combining your accounts	4
45 Helping with deceased estates	219
Total	**3,949**

A major bank reported most of the debt collection breaches. This bank explained that the large number of breaches were reported following enquiries made by the BCCC about the low number of breaches it was previously reporting in this area. In response to these enquires, the bank reviewed and enhanced its processes to better identify and record breaches.

The BCCC will continue to keep banks focused on breach identification and reporting by providing individual feedback to all banks about any concerns that they are not able to identify Code breaches or not being transparent in their reporting to the Committee.

Table 9. Number of breaches reported under Part 9 of the Code, by bank

Bank	Number of breaches
Major bank 1	1,912
Major bank 2	961
Major bank 3	854
Major bank 4	96
Bank A	42

Bank B	29
Bank C	14
Bank D	13
Bank E	7
Bank F	7
Bank G	7
Bank H	3
Bank I	1
Bank J	1
Bank K	1
Bank L	1
Bank M	-
Bank N	-
Bank O	-
Total	**3,949**

The nature and impact of the incidents

Financial difficulty

Banks reported 2,017 breaches of the financial difficulty obligations.

1,000 of these breaches were reported by one major bank and involved an issue where it was charging interest payments on Interest Only loans where a customer had a financial difficulty arrangement in place. The bank manually reversed the payments each month and as such, no financial impact was reported regarding these breaches.

Most of the other breaches involve failures to meet timeframes for communications or decisions on financial difficulty applications or proper consideration of a financial difficulty request.

Debt Collection

Debt collection obligations are set out in Chapter 43 and banks reported 1,703 breaches of these provisions.

The two most common issues were failures to comply with the Debt Collection Guidelines by contacting customers inappropriately or too-frequently and where incomplete or inaccurate file notes were made by staff.

Deceased Estates

The 2019 Code imposes obligations on banks to identify and cease charging fees when notified of a customer's death. Banks are also required to treat the deceased person's representative with respect and compassion and provide clear and concise information on the processes and requirements for dealing with the deceased estate.

Banks reported 219 breaches of these new obligations. The most common issue was a failure to meet timelines after receiving a death certificate and/or probate. The remaining breaches were for providing incorrect information to representatives and failing to refund fees charged after notification of a customer's death.

One notable breach reported by a major bank involved customers being issued with secondary credit cards and communications to cardholders who are deceased. The breach was also reported to ASIC.

What caused the incidents and how they were identified

Banks provided further details of 177 incidents under Part 9 of the Code. The majority of incidents were caused by human error (59%), system error, failure or issue (18%) and control or training issues (14%).

The majority of Part 9 incidents were self-identified by staff (23%) or detected through line 1 monitoring activities (34%). 29% of incidents were identified as a result of a customer complaint (either directly or via AFCA).

How the breaches were corrected

Banks described implementing staff training as the most common action to prevent the recurrence of breaches (57%). For 8% of incidents, banks were conducting ongoing investigations into the incidents, and in 11% no information was provided.

Customer remediation generally took the course of communicating with the customer (20%), apologising (8%) and providing the required information or addressing the individual incident (14%). In a small number of cases (8%), customers were refunded or offered a goodwill payment.

For 19% of cases, banks did not remediate the customer or customer remediation was not required.

Part 10 – Resolving your complaint

Part 10 of the Code 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 1,248 breaches under Part 10 of the Code, a level broadly consistent with the 2,432 breaches reported in 2018-19 on a pro rata basis.

The nature and impact of the incidents

Banks provided further information about 122 incidents primarily related to Part 10 of the Code. As in previous years, about 50% of these incidents related to the late or non-provision of complaint progress or finalisation letters to customers who had made a complaint.

One major bank reported several breaches involving complaints not being entered into the bank's internal system within a timeframe of two days. The same bank also reported breaches which appeared to be related to insurance rather than banking services. There was not enough detail provided about these breaches for the BCCC to determine whether they actually constitute Code breaches, however the bank's reporting shows an encouraging commitment to monitor and report Code-related issues.

Other breaches occurred where a bank:

- failed to record complaints properly
- failed to handle complaints within the specified timeframes, or
- did not provide contact details for AFCA within complaint correspondence.

The total number of customers impacted by complaints handling incidents was 5,279 with a total financial impact of $316,852. Most of this financial impact was from one bank which reported a financial impact of $279,700 for a single breach.

What caused the incidents and how they were identified

70% of incidents were caused by human error, while 12% of incidents were caused by human error, in addition to another cause. 72% of incidents were identified by line 1 monitoring activities or staff self-reporting.

How the breaches were corrected

Banks described implementing one or more of the following corrective actions: Staff training and/or coaching (78%); and process reviews and improvements (7%). Investigations were ongoing for 11% of incidents.

Customer remediation most commonly involved correcting the individual issue (37%), registering a customer's complaint (11%) and/or providing appropriate correspondence (16%). For 22% of incidents, banks reported that no customer remediation was required.

End of Report