BCCC
Banking Code
Compliance Committee

Banks' compliance with the Banking Code of Practice

June – December 2020

August 2021

Contents

Message from the Independent Chair

I am pleased to present the Banking Code Compliance Committee's (BCCC) latest report on Code subscribing banks' (banks) compliance with the Banking Code of Practice (Code).

The BCCC requires banks to report on their compliance with the Code every six months. This report covers banks' self-reported breach data from July to December 2020.

Concerns about an increase in breaches

Banks reported 22,473 breaches for the period – an increase of over 13% compared to 19,766 in the first six months of 2020.

Banks are again reporting that increases in the number of breaches are due to improved monitoring and reporting regimes, although several banks highlighted increased workloads and resource deployments due to the COVID-19 pandemic. The BCCC has previously commented that it has viewed banks' ongoing efforts to build capability to identify and fix non-compliance as a positive development.

The continued improvement of the banks in detecting Code breaches is commendable, as is their support for customers affected by the pandemic. However, the BCCC is concerned that so many breaches of the Code are occurring. Banks need to increase their focus on preventing breaches.

The current version of the Code has now been in operation since July 2019 and it is important for both customers and the standing of banks in the community that the number of breaches starts to decrease.

Positive developments

We are aware of some positive indications that banks are taking actions in this regard.

As part of our feedback process, BCCC staff regularly meet with individual banks for detailed discussions around the banks' compliance data.

At recent meetings, two banks shared examples of where they had examined a particular set of breaches highlighted by us in previous reports, determined the causes, fixed their processes, and eliminated breaches of that nature.

One major bank has indicated that its monitoring and reporting systems have matured over time, and that it may have reached a tipping point where, as it concentrates on improving Code compliance, the number of breaches will start to decrease after years of regular increases.

We look forward to seeing further examples when banks next report on their breach data in September 2021.

Impact of COVID-19 on banks' compliance

As with our previous report, published in April 2021, COVID-19 and its impact on banks and their customers remains a focus for the BCCC. We acknowledge the challenges caused by COVID-19, and while banks breach data does indicate it has had an impact on their compliance with the Code, we also received positive feedback from our Small and Agribusiness Advisory Panel about banks' dealings with small businesses experiencing pandemic-induced hardship during 2020.

In 2021, the Australian Banking Association (ABA) obtained the Australian Securities and Investments Commission's (ASIC) approval to amend the Code in light of concerns that COVID-19 may affect banks internal resources and capacity. The amendments, which came into effect in July 2021, provide some exemptions from strict timing requirements for communications under the Code.

The BCCC required banks to provide information about instances that would have constituted breaches of the timing requirements under the Code but for these exemptions. Nine banks reported 4,651 incidents which may have constituted breaches if not for the exemptions.

Improving data reporting

The BCCC is continuing to engage with the ABA and banks about ways to streamline reporting requirements and the development of additional guidance to improve the consistency and quality of banks breach data.

We will provide further updates about this work in our next compliance report.

Ian Govey AM

Independent Chairperson

Banking Code Compliance Committee

Introduction

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

One of the primary ways the BCCC monitors 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 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.

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 of July to December 2020.

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

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

The BCCC requires banks to report the details of breaches at an incident level 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, but 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.

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

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

Summary of breaches

The 19 banks that subscribe to the Code reported 22,473 breaches of the Code. This represents a 13.7% increase from the previous 6 months.

Table 1 provides a breakdown of the total number of breaches reported by each bank. The four major banks account for nearly 90% of all breaches reported in this period, and Major Bank 1 reported more than 45%.

Table 1. Total number of Code breaches, By Bank, Jul 2019 to Dec 2020

Bank	Jul to Dec 2019	Jan to Jun 2020	Jul to Dec 2020
Major Bank 1	8,811	8,147	10,370
Major Bank 2	1,660	2,926	3,945
Major Bank 3	2,140	3,460	3,460
Major Bank 4	6,128	2,917	2,357
Bank A	506	844	659
Bank B	293	315	421
Bank C	428	292	291
Bank D	161	135	174
Bank E	124	126	162
Bank F	91	106	128
Bank G	106	88	100
Bank H	57	59	99
Bank I	249	117	83
Bank J	32	93	80
Bank K	16	41	68
Bank L	2	27	40
Bank M	47	51	30
Bank N	11	19	5
Bank O	1	3	1
Total	**20,863**	**19,766**	**22,473**

Ten banks reported increases, eighth reported decreases and one major bank reported the same number of breaches as the last period.

The main reasons banks provided for the increases can be summarised as follows:

- Better detection and identification of potential Code breaches as a result of an improved risk culture, employee training and awareness, and increased monitoring activity.
- Following changes made to address COVID-19 impacts, additional volumes of activities and significant numbers of new staff engaged to support customers. Many banks also resumed some activities that were suspended during the initial COVID-19 period. Banks have increased or returned to standard Quality Assurance and monitoring programs to address these changes.
- In some cases, while the number of incidents remained consistent, some banks changed their interpretation and assessment of Code breach incidents.

The Code is made up of 10 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.

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

Table 2. Number of breaches, by Code 'Part'

Code 'Part'	Jan to Jun 2020	Jul to Dec 2020	% change
Part 2 Your banking relationship	8,519	8,740	Up 3%
Part 9 When things go wrong	3,662	4,427	Up 21%
Part 5 When you apply for a loan	2,557	2,877	Up 13%
Part 3 Opening an account and using our banking services	2,019	2,825	Up 40%
Part 10 Resolving your complaint	1,206	1,571	Up 30%
Part 8 Managing your account	821	1,042	Up 27%
Part 4 Inclusive and accessible banking	504	591	Up 17%
Part 6 Lending to small business	316	288	Down 9%
Part 7 Guaranteeing a loan	146	102	Down 30%
Part 1 How the Code works	16	10	Down 38%
Total	**19,766**	**22,473**	**Up 14%**

In accordance with the BCCC's reporting instructions (see **Appendix 1**), banks provided further information about the nature, cause, impact and correction of 2,723 incidents for, constituting 7,533 breaches – 34% of the total reported. The rest of this section of the report refers only to this subset of incidents.

Cause of breaches

Banks reported that the majority of incidents (69%) were caused by human error alone, and a further 3% caused by human error plus another factor. These figures are consistent with the previous six-month reporting period.

14% involved a control, training or resourcing failure (including process deficiencies) and 8% involved a system error.

Breach identification

Banks identified 30% of incidents via 'Line 1' quality assurance activities including call monitoring and system monitoring. 29% were identified as a result of customer complaints, queries or feedback.[1]

The other most prominent method of breach identification was self-identification by staff members not specifically involved in line 1 activities (24%).

A further 10% of incidents were identified by line 2 or internal reviews and 3% via external parties or events.

Impact

Overall the sample of incidents reported for July to December 2020 affected more than 2.8 million customers, with a total financial impact of over $76 million.

Customer remediation and corrective actions

The BCCC collects data about how banks both 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:

- provide staff training, coaching or feedback (60% of incidents)
- review and/or improve processes (14%)
- review staff performance or taken disciplinary action (8%).
- implemented a system fix (6%), and
- enhance monitoring or controls (3%).

Bank actions to prevent recurrence were still under review at the time of reporting for 7% of incidents. Banks did not provide details of efforts to prevent recurrence for 6% of incidents.

[1] Refer to **Appendix 1** for more information about the 'three lines of defence'.

Banks reported that they did not take actions to prevent recurrence or no action was required for approximately 3% of incidents.[2]

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

- corrected the individual issue, including updating details, and requests for information be destroyed, deleted or returned (55% of incidents)
- provided financial remediation such as a refund, debt waiver, compensation or goodwill payment (20%)
- communicated or corresponded with the customer (10%)
- apologised to the customer (10%), and
- logged, managed or resolved a complaint (3%).

Banks reported there was no customer remediation provided or customer remediation was not required for 9% of incidents. For 11% of incidents, the matter was 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 2% of incidents or confirm that these breaches were still under investigation. While this is less than the 5% for the previous six-month period, the BCCC will continue to provide feedback to the banks involved to ensure that complete information is provided in future reporting.

Review of the consistency of breach reporting

As noted in the BCCC's last compliance report, the ABA has been working with its member banks to review of the way they classify and report Code breaches.

This review comes after several years of the BCCC raising concerns about the consistency and quality of data provided by banks in the Compliance Statement. The BCCC has stated often that it is concerned about the discrepancies in numbers of overall breaches reported by banks, and the way in which they classify and report them.

The review was in progress at the time of preparing this report and the BCCC will report on any further developments in its next compliance report.

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

Update on COVID-19 and scam and fraud related breaches

COVID-19

As with our previous compliance report, the BCCC has sorted and classified Code breaches where banks explicitly noted they were related to or in some way caused by the effects of the pandemic.

In this reporting period, twelve banks reported a total of 230 breaches of this kind. These breaches affected more than 200,000 customers with an overall financial impact of over $1.7 million. Several of the most impactful breach incidents related to small business customers.

Many breaches were where banks had not sent required notifications to customers, or there were delays in doing so. There were also a number of processing errors related to banks' COVID-19 assistance packages, affecting individuals and small businesses, for instance:

- Customers placed on assistance packages without being asked
- Processing errors when placing customers on, and exiting them from, COVID-19 assistance packages
- Customers automatically declined for assistance due to systems deficiencies
- Checks not being performed if customers' situations or income were affected by COVID-19, thus potentially missing opportunities to assist
- Collections activity and default listings applied to customers on COVID-19 assistance

Banks generally attributed these incidents to the high volume of requests, and in implementing system changes across large tranches of customers and account types.

We expect that banks' systems and processes will have matured over the reporting period and as these new processes bed in, COVID-related breaches will decline. The BCCC has included the challenges caused by the COVID-19 pandemic, including financial difficulty, as priority areas for the BCCC monitoring activities in its 2021-22 Business Plan.

Special Note

The pandemic greatly increased the number of customers reaching out to their banks for assistance. Anticipating this increased workload, the ABA sought ASIC's approval to

amend the Code by including a Special Note which provides some exemptions from strict timing requirements for notices and communications under the Code.

Banks were required to notify customers that there may be delays in processing their requests for hardship assistance, and if this notification was given, and banks made reasonable efforts to meet the timelines, the delays would not be recorded as a breach of the relevant Code chapter(s).

The Special Note took effect from 1 July 2020 and applied for the whole of the current reporting period.

The BCCC required banks to provide information about instances that would have constituted breaches of the following timing requirements under Code, but for the COVID Special Note:

- 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, and
- 205 and 206 – complaints handling timeframes.

This request was made with reference to Paragraph 5 of the Explanatory Memorandum for the *ASIC Corporations (Approval of Variation of March 2020 Banking Code of Practice) Instrument 2020/602*. [3]

Nine banks recorded a total of 4,651 such incidents. Two banks recorded the majority and the other seven reported only a small percentage.

Banks were not required to provide details of the incidents, but nearly all of the incidents were related to Chapter 39 – *Contact us if you are experiencing financial difficulty*.

The Special Note also required banks to advise customers of the possibility of delays when acknowledging a complaint. Several banks were confident that they would still be able to meet the complaints handling timelines required by the Code and did not wish to warn customers of a delay that would not occur. These banks sought exemptions from the Special Note. The BCCC granted exemptions on condition that these banks reported all breaches and incidents where the Code's complaints handling timeframes were not met.[4]

[3] "*Also in relation to the Timing Requirement Wording, Code-subscribing banks have made a commitment to ASIC that they will track instances that would, but for the COVID-19 Special Note, have constituted breaches of the relevant timing requirements and provide information about these to the Banking Code Compliance Committee (BCCC) upon request. This commitment is intended to enable the BCCC, as the Code's monitoring body, to maintain oversight over banks' performance under the Code during the period of the COVID-19 Special Note.*"

[4] BCCC Guidance Note No. 3: Complaints handling timeframes and customer notifications, September 2020.

Scams and fraud

In our last compliance report we described some of the most common scams and the ACCC's reports on scams.[5]

As with COVID-19 related breaches, the BCCC analysed all incident reports from banks and flagged breach incidents where a scam or fraud was involved.

We identified more than 280 breaches of this kind and again while this is not an unduly large number, this is an increase on the number included in the last compliance report and the incidents are often of a serious nature. These breach incidents affected over 500 customers and had a financial impact of nearly $6 million.

Examples of incidents related to scams and fraud include:

- customers who were experiencing vulnerability making repeated payments to scammers but did not receive extra care and scrutiny of the transactions by staff
- branch staff not asking additional questions when a customer requested a large international transfer that turned out to be to share trading scam
- a vulnerable customer being a victim of a fraud by a family member
- phone and internet transfers where a person impersonates the customer, sometimes via "phone-porting" whereby a phone is copied by criminals
- calls from scammers claiming to be from a bank's fraud team and asking customers to disclose online access details
- elder abuse and misuse of Power of Attorney
- employees not completing identification/ 'know your customer' processes correctly, resulting in fraudulent withdrawals from accounts.
- employees not acting on customers' concerns about fraudulent transactions, or overriding restrictions where banks' fraud teams had flagged accounts

We again observed a number of cases where customers started making unusually large withdrawals/transfers from accounts or funds being fraudulently removed from accounts and staff and/or systems did not recognise or raise the potential red flags in these transactions.

Many of the incidents reported in this period were related to customers' identity being taken over by criminals. In many cases this appears to have been via scammers tricking customers into providing their internet/phone banking credentials, and the criminals then withdrawing large amounts of money electronically.

The BCCC continues to encourage banks to ensure that systems and processes are as robust as possible, and employee awareness of fraud and scam issues is promoted to help protect customers and the banks themselves from scammers and other criminal enterprises.

[5] BCCC Report: Banks' compliance with the Banking Code of Practice – January to June 2020, April 2021

Banks' compliance with the Banking Code

The BCCC has 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

Part 2 of the Code contains Chapters 3 to 7. Banks reported a total of 8,740 breaches of Part 2, comprising:

- Chapter 3 – Our compliance with this code – 6 breaches
- Chapter 4 – Trained and competent staff – 4,564
- Chapter 5 – Protecting Confidentiality – 4,165
- Chapter 6 – Compliance with laws – 4
- Chapter 7 – Closing a branch – 1

Banks provided further information about the nature, cause, impact and correction of 1,517 incidents related to Part 2. The rest of this section of the report refers only to this subset of incidents and associated breaches.

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.

In some cases, Chapter 4 appears to be used as a 'catch-all' when classifying some breach incidents, and it is difficult to summarise the types of incidents that are reported as a breach of Chapter 4. They effectively include every type of incident for which a primary breach might be reported under any other Code obligation, ranging from lending and financial difficulty matters to privacy and account processing issues.

Some of the most impactful breaches in terms of the number of customers affected and the total financial impact are reported as breaches under Chapter 4, including incorrect interest and fee charges and transaction errors.

However, as the BCCC has commented on elsewhere in this report and in previous reports, banks tend to:

- blame human error for breaches where better systems (IT and processes) may have prevented staff from making the error, and
- over-rely on staff training and feedback to prevent recurrence where improvements to systems and controls might be more effective.

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 4,165 breaches reported for this period.

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

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

While banks reported that the majority of privacy and confidentiality breaches did not have a financial impact on customers, several breaches were of the types described above.

There was a decrease in incidents related to bank staff working from home, such as using personal emails and exposing customer information to family and housemates. We consider that this is likely a result of banks and their staff implementing safer home working processes and being more aware of the potential risks.

69% of privacy and confidentiality incidents were classified as being caused by human error. Banks should be acting to prevent these types of issues with appropriate systems controls.

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 2,826 breaches of Part 3 obligations in total and further details 340 incidents (or 699 breaches). The breaches were generally related to banks providing incorrect or misleading information or advice to customers, and incorrect fees charges and interest rates. A number of these breaches occurred when terms and conditions or special offers were unclear, and staff gave customers incorrect advice.

Breaches of Part 3 obligations affected more than 1.4 million customers and some breaches had a significant financial impact where there was a discrepancy between a bank's terms and conditions and actual fees or interest charges. Breaches of this nature are more often reported as a breach under Part 2 of the Code.

Banks reported that most of the incidents (48%) were the result of human error. 21% were the result of a deficient process or procedure. Banks identified Part 3 incidents following complaints from the customer in 31% of cases, followed by Line 1 monitoring (26%).

Banks provided financial remediation to customers for 20% of these Part 3 breach incidents. Banks' corrective actions to prevent further breaches were predominantly through staff training, coaching or feedback (36%).

Part 4 – Inclusive and accessible banking

Part 4 of the Code contains Chapters 13 to 16. It 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.

The BCCC considers Part 4 to be a priority for its monitoring activities and will shortly report on an inquiry it has been conducting into banks' compliance with these provisions.

Banks reported 591 breaches overall of Part 4 of the Code for this period – a 17% increase from the previous six months. Eight banks did not report any breaches of obligations under Part 4.

Nearly half of the breaches were reported by Major Bank 1. That bank attributed the increase in these breaches to improvements to monitoring activities and the impacts of the pandemic and bushfires leading to an increased number of customers experiencing vulnerability contacting the bank for assistance.

Banks provided further information about the nature, cause, impact and correction of 46 incidents related to Part 4.

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

- failure to identify and take extra care with customers who may be experiencing vulnerability
- customers on low incomes not offered no-fee accounts, and
- failure to take extra care with vulnerable customers who are subjected to scams or fraud.

Other issues included errors made in dealing with a Power of Attorney and account processing issues.

Banks reported that most of the incidents (72%) were the result of human error and 52% of Part 4 incidents were identified following complaints from the customer. The data shows Part 4 Incidents are identified from customer complaints at a higher rate than for other parts of the Code. The BCCC's Part 4 inquiry report will include further information about banks' approach to monitoring activities across branches, contact centres and digital channels.

Part 5 – When you apply for a loan

Part 5 of the Code includes Chapter 17 to 19, which contain the provisions relating to responsible lending.

Banks reported 2,877 breaches overall of Part 5 of the Code for this reporting period.

2,860 of the Part 5 breaches were of Chapter 17, with 17 breaches of the other chapters covering the selling of consumer credit insurance (CCI) and lenders' mortgage insurance. Examples of the CCI breaches related to the availability of claims information on a bank's website and sending incorrect annual reminder notices.

Banks provided further information about the nature, cause, impact and correction of 232 incidents related to Part 5. Those incidents represent a total of 778 breaches.

Chapter 17, *A Responsible approach to lending*, was the Chapter with the fourth highest number of breaches for this reporting period.

Major Banks 1 and 4 each reported approximately 40% of all Chapter 17 breaches for this period. Five banks did not report any breaches of Part 5 or Chapter 17.

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

- credit assessments being incomplete, unsatisfactory, or using inaccurate or unverified information
- the loan being unserviceable, unaffordable or unsuitable, and
- co-borrower benefits not being assessed.

Banks reported that most of the incidents (81%) were the result of human error – a higher percentage than for breach incidents across the whole Code. Banks identified 40% of Part 5 incidents by line 1 monitoring activities and 23% were identified as a result of customer complaints.

Part 6 – Lending to Small Business

Part 6 of the Code contains Chapters 20 to 24. It includes banks' obligations when specifically lending to small business customers. Chapter 20 describes banks' obligations in assisting small business customers applying for a loan, including information to be provided, and banks' obligations to keep small business customers informed of the progress of their application.

Banks reported 288 breaches overall of Part 6 of the Code, a small decrease on the previous period, when 316 breaches were reported. Major Bank 3 accounted for 94% of the breaches under Part 6.

One of the incidents, where pre-application disclosure documents were not provided via email, affected 200 small business customers and was reported as 200 separate breaches of Chapter 20. The same bank reported 20 breaches where it failed to issue a notice of a decision not to extend a loan.

Part 7 – Guaranteeing a loan

Part 7 of the Code contains the obligations for guaranteeing a loan and 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 information prior to entering into a guarantee, and there are strict conditions around the signing of a guarantee.

The BCCC recently published a report of its major Inquiry into banks' compliance with guarantee obligations and highlighted concerns about effective record management practices, inadequate or ineffective monitoring of compliance controls and guarantee-related data capabilities. [6]

Banks reported 102 breaches overall of Part 7 of the Code for this reporting period. Banks provided further information about the nature, cause, impact and correction of 29 incidents related to Part 7. Those incidents represent a total of 56 breaches.

Table 3: Breakdown of Part 7 Code breaches, By Chapter

Code Chapter	Number of breaches
25 Limiting liability under the guarantee	5
26 What we will tell and give you	69
27 Signing your guarantee	18
28 Withdrawing or ending your guarantee	10
29 Enforcing our rights under the guarantee	0
Total	**102**

Incidents reported by banks included:

- not providing the three-day period before the signing of a guarantee
- incorrect or incomplete information being provided to guarantor
- information not provided to guarantor or provided to the wrong party, and
- information about the financial difficulties of a borrower not provided to guarantor.

Banks reported that most of the incidents (62%) were the result of human error and banks identified Part 7 incidents in 45% of cases through line 1 monitoring activities.

[6] *BCCC Inquiry Report: Banks' compliance with the Banking Code's guarantee obligations*, August 2021

In most cases the remediation involved providing the required information to the customer. In one case where the customer had complained to AFCA, the customer was provided compensation for non-financial loss and released from the guarantee.

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 1,042 breaches of Part 8 of the Code for this period.

Table 4: Breakdown of Part 8 Code breaches, By Chapter

Code Chapter	Number of breaches
30 Keeping your accounts safe and secure	11
31 Statements we will send you	15
32 Cost of transaction service fees	22
33 Managing a credit card	7
34 Direct debits and recurring payments	448
35 Joint Accounts	81
36 Closing any of your banking services	332
37 Your right to copies of certain documents	15
38 When we change our arrangements with you	32
Total	**1,042**

Banks reported a wide range of incidents as breaches under Part 8 and more than 200,000 customers were affected by these breaches.

Chapter 34 - *Direct debits and recurring payments* had the highest number of breaches in Part 8. Some examples include banks not following customer instructions in relation to actioning a direct debit or cancelling a direct debit. The BCCC has conducted further monitoring activities into this issue because of historic and ongoing concerns about banks' compliance with these obligations. We will report on the findings in due course.

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 4,427 breaches overall of Part 9 of the Code. This represents a 21% increase from the previous six month reporting period. Increases in debt collection and deceased estate breaches account for the majority of the increase overall. Breaches of Chapter 43 - *When we are recovering a debt* increased nearly 40% this period.

The increase in breaches of Chapter 43 was primarily attributed to increases in the following:

- levels of collections activity related to COVID-19
- numbers of new staff members supporting customers, and
- quality assurance activities to monitor customer interactions.

Table 5: Breakdown of Part 9 Code breaches, By Chapter

Code Chapter	Number of breaches	
	Jan–Jun 20	Jul-Dec 2020
39 Contact us if you are experiencing financial difficulty	1,004	303
40 We may contact you if you are experiencing financial difficulty	14	24
41 We will try to help you if you are experiencing financial difficulty	392	1086
42 When you are in default	112	59
43 When we are recovering a debt	1,886	2,635
44 Combining your accounts	13	2
45 Helping with deceased estates	241	318
Total	**3,662**	**4,427**

Breaches of Part 9 obligations affected over 38,000 customers.

Nine breaches were systemic in nature and affected over 30,000 customers. One debt collection breach affected over 18,000 customers and involved the bank sending incorrect debt assignment notices.

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

- Requests for financial difficulty assistance not considered or not considered within timeframes
- Financial difficulty triggers not identified
- Debt collection breaches such as:
  - Inappropriate contact
  - Providing incorrect or misleading information
  - Record keeping deficiencies
  - Collections activity during an AFCA complaint or where a hardship arrangement was in place
  - Failure to inform customers that their debts had been sold to third party

- Deceased Estate delays and errors

One major bank reported the majority of the deceased estates breaches and this involved an issue with a manual process for frontline staff to process requests received in branches in a timely manner. Frontline staff are required to create and send the relevant correspondence in the bank's system to the correct internal team for action. There were approximately 400 to 500 requests created per week. The bank has put additional controls in place and is developing an automated process to improve the timeliness of the process.

Banks reported that most of the incidents under Part 9 (72%) were the result of human error. Nearly 60% of incidents were identified through line 1 monitoring activities.

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 1,571 breaches overall of Part 10 of the Code for the period July to December 2020 – a 30% increase when compared to the 1,206 breaches for the last six-month period.

Overall the data indicates there were no large scale systemic failings regarding complaints handling during the reporting period. Banks provided details of 174 incidents that affected 1,782 customers in total. Where banks provided further details of the incidents, most breaches were related to complaints handling delays or staff failing to register customers' complaints when they expressed their dissatisfaction.

One major bank reported a breach where it had passed on costs relating to the management of AFCA complaints to customers in a small number of cases due to a flaw in its process. The bank was working to remediate customers and implement a permanent fix to the issue at the time of reporting.

Banks reported that most of the incidents (92%) were the result, at least in part, of human error. Consequently, banks reported that they corrected breaches predominantly through staff training, coaching or feedback (88% of incidents).

To remediate the breaches banks most often log and manage a complaint and communicate with the customer or complainant.

Banks identified Part 10 incidents following line 1 monitoring activities 72% of the time. Staff self-reported the incidents in 12% of cases.

Appendix 1: About the BCCC and the Compliance Statement

The BCCC

The BCCC is an independent monitoring body established under clause 207 of the Code. Its purpose is to monitor and drive best practice Code compliance. To do this, the BCCC:

- examines banks' practices
- identifies current and emerging industry wide problems
- recommends improvements to bank practices
- sanctions banks for serious compliance failures, and
- consults and keep stakeholders and the public informed.

The BCCC's 2021–24 Strategic Plan sets out its overall objectives to fulfil its purpose to monitor and drive best practice Code compliance. The BCCC's 2021–22 Business Plan sets out the priority areas and activities it will undertake to meet the objectives in the Strategic Plan.

The following represent the priority areas that the BCCC will likely focus on in 2021–22:

- Challenges caused by the COVID-19 pandemic, including financial difficulty
- Customers experiencing vulnerability
- Small business and farming customers
- Banks' organisational capability to comply with the Code
- Deceased estates
- Banks' communications with customers and provision of information

The BCCC has published Operating Procedures which provide guidance about how the BCCC conducts its monitoring activities. One of the primary ways the BCCC monitors banks' compliance with the Code is through the Banking Code Compliance Statement.

The BCCC activities are determined with reference to its Code Monitoring Priority Framework.

Further information about the BCCC and members of the Committee is available on the BCCC's website - bankingcode.org.au.

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.

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

The BCCC requires 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, the BCCC has 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.[7]

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