BCCC
Banking Code
Compliance Committee

Banks' compliance with the Banking Code of Practice

January – June 2021

March 2022

Contents

Independent Chair's Message

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 January to June 2021.

A separate report in relation to comprehensive Part B data provided for the first time in full by banks for the 2020-21 reporting period will be published at a later date.

An overall decrease in breaches

Banks reported 20,605 breaches for the period, approximately a 10% decrease from the previous six-month period where they reported 22,876 breaches.

The decrease in breaches was largely driven by Major Bank 1 reporting a 38% decrease, from 10,370 to 6,413. As reported previously, this bank said its monitoring and reporting systems for Code compliance have matured so that it is confident it is detecting every Code breach, and is now re-allocating resources to preventing breaches.

Major Bank 4 reported a 10% decrease from the previous reporting period, from 2,357 to 2,131.

Seven other banks (Banks A, B, C, E, H, J, K) reported a decrease in breaches compared to the previous reporting period.

Increase in breaches for some banks

Major Bank 2 reported a 50% increase in breaches from the previous reporting period, from 3,945 to 5,935. This bank reported that ASIC's more stringent reporting requirements, along with maturing compliance regimes and the ongoing effects of the pandemic, drove increases in monitoring and therefore detection.

Major Bank 3 reported a 5% increase from the previous reporting period, from 3,863 to 4,054.

Six other banks (Bank D, F, G, I, L, N) reported an increase in breaches compared to the previous reporting period, while two other banks (Bank M, N) reported the same number of breaches for both periods.

Industry Trends

While the overall 10% decrease is a positive development, there is further work to be done and room for improvement.

One bank reported a large drop in the number of its privacy breaches. Based on feedback we provided in previous reporting periods, the bank improved some of its systems and staff awareness, leading to a drop in both the number and seriousness of privacy breaches.

As with the large reduction in breaches reported by Major Bank 1, these results show the value of the BCCC's breach data collection and reporting. I encourage all banks to note the feedback we provide them individually, as well as the improvements being made by their co-subscribers.

Impact of COVID-19 on banks' compliance

As with our previous reports, published in April and August 2021, COVID-19 and its impact on banks and their customers was a key focus for the BCCC.

The COVID-19 Special Note remained in place for this reporting period. 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. Five banks reported 1,481 incidents which may have constituted breaches if not for the exemptions, a significant reduction on the 4,651 incidents reported in the previous period.

Several banks reported breach incidents where customers on COVID-19 deferral packages, or customers who had exited the packages, were not quarantined from other bank systems. For example, many customers were sent default notices or were referred to banks' recovery departments while they were on a deferral package. Many customers who had exited the deferrals remained on banks' hardship systems.

These errors would have caused distress to the customers involved and may have impacted their credit ratings.

Our analysis of these incidents indicates that overall banks worked hard to assist customers affected by the pandemic and rapidly deployed human and IT resources to that end. However, many of their internal systems were not concurrently updated.

Improving data reporting

The BCCC is continuing to engage with the Australian Banking Association (ABA) and banks about ways to streamline reporting requirements and develop additional guidance to improve the consistency and quality of banks' breach data.

Breach data was examined in both the Banking Code and BCCC Reviews. The BCCC will consult with stakeholders in relation to the recommendations made on this issue.

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 from January to June 2021.

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 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 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 overall

The 19 banks that subscribe to the Code reported 20,605 breaches of the Code. This represents a 10% decrease from the previous six months.

One of the Major Banks reported additional breaches almost three months after the due date for submission of breach data for the reporting period of Jul-Dec 2020. The BCCC has decided not to include these additional breaches in the totals reported below to enable accurate reporting for this period. As a result, the total breaches for the reporting period of Jul-Dec 2020 cited in this report will differ from our previous report.[1]

Table 1 provides a breakdown of the total number of breaches reported by each bank. The four major banks account for 90% of all breaches reported – as can be seen, there are significant movements compared to the last period. Major Bank 1 recorded a decrease of 38% and Major Bank 2 recorded an increase of 50%.

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	Jan to Jun 2021
Major Bank 1	8,811	8,147	10,370	6,413
Major Bank 2	1,660	2,926	3,945	5,935
Major Bank 3	2,140	3,460	3,863	4,054
Major Bank 4	6,128	2,917	2,357	2,131
Bank A	506	844	659	546
Bank B	293	315	421	306
Bank C	428	292	291	287
Bank D	161	135	174	175
Bank E	124	126	162	145
Bank F	106	88	100	115

[1] While it is encouraging to see that the bank reported these breaches, banks are required to report their breach data in a timely manner.

Bank G	57	59	99	111
Bank H	249	117	83	81
Bank I	16	41	68	71
Bank J	32	93	80	70
Bank K	91	106	128	69
Bank L	47	51	30	51
Bank M	2	27	40	40
Bank N	11	19	5	5
Bank O	1	3	1	0
Total	20,863	19,766	22,876	20,605

Seven banks reported increases, nine reported decreases, two banks reported the same number of breaches and one bank reported no Code breaches.

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

- Better detection and identification of potential Code breaches due to improved risk culture, employee training and awareness, and increased monitoring activity.
- In response to ASIC's more stringent reporting requirements, some banks greatly improved monitoring across their businesses and this resulted in significant increases across some Code chapters.
- Banks continue to develop their monitoring and reporting systems and improve their compliance, and some increases and decreases in reported breaches have been attributed to this evolution.

Major Bank 1 explained the 38% decrease is a result of the bank investing heavily in systems, processes and people to monitor for and detect Code breaches. The bank is confident that it is detecting every breach of the Code and has been focussing resources from detection to prevention.

Another bank reported that its breaches of Chapter 5 (Protecting confidentiality) were reduced by half, in large part due to BCCC feedback over previous Compliance Statement Reports.

Code breaches by Part

The Code is made up of 10 Parts. Each Part of the Code comprises Chapters which detail obligations about service standards for specific aspects of a customer's banking experience or for a specific type of customer.

Table 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	Jul to Dec 2020	Jan to Jun 2021	% change
Part 2 Your banking relationship	8,789	7,139	Down 19%
Part 9 When things go wrong	4,434	4,152	Down 6%
Part 3 Opening an account and using our banking services	3,060	3,442	Up 12%
Part 5 When you apply for a loan	2,898	2,076	Down 28%
Part 10 Resolving your complaint	1,629	1,434	Down 12%
Part 8 Managing your account	1,070	1,299	Up 21%
Part 4 Inclusive and accessible banking	596	651	Up 9%
Part 6 Lending to small business	288	292	Up 1%
Part 7 Guaranteeing a loan	102	120	Up 18%
Part 1 How the Code works	10	0	Down 100%
Total	**22,876**	**20,605**	**Down 10%**

Significant movements

Breaches of Part 8, relating to the management of account appear to have increased by 21% largely due to banks' failure to action customers' accounts in accordance with their instructions. Examples include failure to action direct debit cancellation request, failure to action account closure request and customers switched to receive statements electronically when they did not have access to internet banking.

Breaches of Part 5 appear to have decreased by 28% and banks have generally explained that better compliance has led to this reduction.

Statistics used in this report

In accordance with the BCCC's reporting instructions (see **Appendix 1**), banks provided further information about the nature, cause, impact and correction of 2,761 incidents, constituting 7,269 breaches – 35% 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 most incidents (69%) were caused by human error alone, and a further 3% were caused by human error plus another factor. These figures are consistent with the previous six-month reporting period.

We are concerned that banks are continuing to identify human error as the cause of the majority of Code breach incidents. Our analysis of many incidents attributed to human error indicates that better systems and processes, along with better controls and oversight could have prevented the breaches from occurring.

The BCCC's Report, Building Organisational Capability, published early last year, highlights the need for banks' compliance frameworks to include sufficient measures to prevent human error related breaches from recurring. The BCCC encourages banks to ensure such measures are incorporated into their compliance frameworks. An uplift in systems and processes, improved controls and greater oversight by banks will assist in prevention of breaches and reduce the possibility of human error.

Breach identification

Banks identified 33% of incidents via customer complaint, query or feedback. A further 32% were self-reported by staff and/or immediate managers. 'Line 1' quality assurance activities including call monitoring and system monitoring detected 18% of breaches.[2]

Another 10% of incidents were identified by line 2 or internal reviews and 3% via Line 3 internal audits.

Impact

Overall the sample of incidents reported for January to June 2021 affected more than 2.5 million customers, with a total financial impact on customers of over $56 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 (58% of incidents)
- review and/or improve processes (14%)
- review staff performance or taken disciplinary action (6%).
- implemented a system fix (6%), and
- enhance monitoring or controls (5%).

Bank actions designed to prevent recurrence were still under review at the time of reporting for 7% of incidents.

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

As with banks' reliance on human error as a cause of breach incidents, it appears that staff training is overly relied upon as a corrective action. Obviously, better-trained staff make fewer errors, but improved systems, processes and controls are key to decrease the risk of Code breaches and other errors.

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

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 (41% of incidents)
- provided financial remediation such as a refund, debt waiver, compensation or goodwill payment (18%)
- communicated or corresponded with the customer (10%)
- apologised to the customer (5%), and
- logged, managed or resolved a complaint (5%).

Banks reported customer remediation was not provided or required for 3% of incidents. For 16% of incidents, the matter was still under investigation at the time of reporting or banks had yet to consider customer remediation.

Banks did not provide details of remediation activities for less than 1% of incidents or confirm that these breaches were still under investigation. This shows a year on year improvement in this area and we commend banks for responding to our feedback on this issue.

Review of the consistency of breach reporting

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

The review was completed by the time this report was prepared and the BCCC is working with banks to act on the recommendations of the review.

In response to the review, the BCCC commenced its compliance statement consultation with banks and work in this area is ongoing. The aim of the consultation is to streamline data reporting requirements to achieve greater consistency and align reporting with ASIC's data dictionary categories.

Breach reporting is also considered in the recently published Banking Code and BCCC Review reports and the recommendations in relation to this issue will be examined in further detail in the coming period.

[3] 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 reports, the BCCC has 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, eight banks reported a total of 107 breaches of this kind. These breaches affected nearly 60,000 customers with an overall financial impact of over $3 million. In the last period, 12 banks reported 230 breaches affecting over 200,000 customers with a financial impact of $1.7 million.

Breaches of this kind generally appeared to be caused by processing errors related to banks' COVID-19 assistance packages, affecting individuals and small businesses, for instance:

- Errors when placing customers on, and exiting them from, COVID-19 assistance packages
- 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. Analysis of these breaches indicates that some banks' automated systems have not kept up with the rapidly-developed COVID-19 assistance packages they implemented.

Fewer breaches involved the placement or non-placement of customers on COVID-19 assistance packages, but many customers found themselves caught by banks' automated default and collections systems when they should have been quarantined.

COVID-19 Special Note

The pandemic greatly increased the number of customers reaching out to their banks for assistance. In anticipation of the increased workload, the ABA obtained 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.

The Special Note took effect from 1 July 2020 and applied for 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-19 Special Note[4]:

- 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.

Five banks recorded a total of 1,481 such incidents, a significant decrease in the totals from the previous reporting period. One bank recorded 1,201 incidents, another reported 215 and the other three reported the remaining 47. In the previous period, eight banks reported 4,651.

Banks were not required to provide details of the incidents, but nearly all 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.[5]

Scams and fraud

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 63 incidents of this kind and while this is not an unduly large number, many of the incidents were of a serious nature. These breach incidents affected over 170 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
- phone and internet transfers where a person impersonates the customer, sometimes via "phone-porting" whereby a phone is copied by criminals
- elder abuse and misuse of Power of Attorney, and
- employees not completing identification/ 'know your customer' processes correctly, resulting in fraudulent withdrawals from accounts.

[4] 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. *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."*

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

Many of the incidents were related to customers' identities being taken over by criminals (identity theft). In some cases this appears to have been via scammers tricking customers into providing their internet/phone banking credentials, followed by large withdrawals of funds conducted electronically by the fraudsters. We also saw a slight rise in the number of frauds perpetrated by mobile phone or SIM "porting" or cloning.

The incidents with the largest financial impact on customers, in some cases hundreds of thousands of dollars, related to abuse of Power of Attorney and Elder Abuse, and customers caught up in investment scams.

One incident of note had a reported financial impact of over $2 million. It involved a staff member accessing their family members' funds and was still under investigation at time of writing.

For the first time we have included incidents of staff misconduct in our Fraud figures – some relate to staff 'gaming' their KPIs for their own benefit, but there were also more serious incidents involving staff preparing and processing fraudulent loan documents. In one case a staff member allowed a loan package to proceed in circumstances where the co-borrower was presumably unaware of the application and the documents were clearly forged by the borrower.

The BCCC continues to encourage banks to ensure that systems and processes are as robust as possible, and that both employee and customer awareness of fraud and scam issues is promoted to help protect customers and the banks. This is particularly important and topical during this period of time when scams are widespread and fraud in general is so prevalent and continues to be on the rise.

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 includes a more detailed examination of specific chapters and sections where necessary.

Part 2 – Your Banking Relationship

Banks reported a total of 7,139 breaches of Part 2, comprising:

- Chapter 3 – Our compliance with this code – 0
- Chapter 4 – Trained and competent staff – 2,474
- Chapter 5 – Protecting Confidentiality – 4,662
- Chapter 6 – Compliance with laws – 1
- Chapter 7 – Closing a branch – 2

Banks provided further information about the nature, cause, impact and correction of 1,289 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.

It remains the case, that in some instances, 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.

However, as the BCCC has commented 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.

The BCCC encourages banks to classify breach incidents as accurately as possible.

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 4,662 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.

One Major Bank reported a 20% increase in breaches relating to Chapter 5. The bank said it is currently making overall enhancements to its Privacy Framework and developing targeted training to address this increase. The bank noted that the breaches were predominantly caused by human error.

Overall, 87% of privacy and confidentiality incidents were classified as being caused by human error. Banks should be more proactive in preventing these types of breaches with appropriate systems and controls.

Part 3 – Opening an account and using banking services

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

Banks reported 3,442 breaches of Part 3 obligations in total and further details of a sample of 524 incidents. The breaches were generally related to unclear terms and conditions and banks providing incorrect information to customers.

Breaches of Part 3 obligations affected more than 1.4 million customers.

Banks reported that the majority of these incidents, 55%, were the result of human error and 20% were the result of a deficient process or procedure. Banks identified Part 3 incidents as a result of complaints from the customer in 40% of cases, followed by 22% self-identified or reported by a staff member.

Banks provided financial remediation to customers for 26% of these Part 3 breach incidents. Banks' corrective actions to prevent further breaches were predominantly through staff training, coaching or feedback 49%.

Part 4 – Inclusive and accessible banking

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

Banks reported 651 breaches overall of Part 4 of the Code for this period – an 9% increase from the previous six months. Five banks did not report any breaches of obligations under Part 4.

Half of the breaches were reported by Major Bank 2. That bank attributed the increase in these breaches to the increased level of monitoring, internal reviews and staff training.

Banks provided further information about the nature, cause, impact and correction of 66 incidents related to Part 4.

The nature of the incidents banks reported remain the same as the previous reporting period:

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

Banks reported that most incidents,71%, were the result of human error and 58% of Part 4 incidents were identified following complaints from the customer. Identification of Part 4 incidents via customer complaints remains at a higher rate than for other parts of the Code.

The BCCC's Part 4 Vulnerability, inclusivity and accessibility inquiry report published on 20 December 2021 provides further information about banks' approaches to monitoring activities across branches, contact centres and digital channels. We strongly recommend that banks consider the content of this report including the good practise examples to provide more inclusive and accessible banking products and services and in taking extra care to assist with customers experiencing vulnerability. We believe that adoption of good practice in relation to these obligations should correspond with a decrease in the overall amount of breaches of this Part of the Code.

Part 5 – When you apply for a loan

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

Banks reported 2,076 breaches overall of Part 5 of the Code for this reporting period.

1,987 of the Part 5 breaches were of Chapter 17, with 89 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 283 incidents related to Part 5. Those incidents represent a total of 754 breaches.

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

Major Bank 4 reported approximately 42% of all Chapter 17 breaches for this period, followed by Major Banks 1 and 2 with each reporting over 20%. Five banks did not report any breaches of Part 5.

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 81% of the incidents were the result of human error. Banks identified 33% of Part 5 incidents by line 1 monitoring activities and 25% as a result of customer complaints.

Part 6 – Lending to Small Business

Part 6 of the Code (Chapters 20 to 24) includes banks' obligations when 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 their obligations to keep small business customers informed of the progress of their application.

Banks reported 292 breaches of Part 6, a 1% increase on the previous period, when 288 breaches were reported. Major Bank 3 accounted for 96% of the breaches under Part 6.

One of the incidents, where pre-application disclosure documents were not provided, affected 286 small business customers and was reported as 275 separate breaches of Chapter 20. The same bank failed to issue a key general terms and conditions of the loan summary document to 16 small business customers.

As with individual customers, many small business customers continue to feel the impacts of COVID-19. During this period, where many small businesses have experienced an increased need for additional finance, it is important that banks continue to assist small business customers when applying for a loan and provide information relating to loan applications in accordance with their Part 6 obligations.

Part 7 – Guaranteeing a loan

Part 7 of the Code (Chapters 25 - 29) contains the obligations for guaranteeing a loan and some of the most prescriptive requirements within the Code. It includes 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.

Banks reported 120 breaches overall of Part 7 of the Code for this reporting period. Banks provided further information about the nature, cause, impact and correction of 30 incidents related to Part 7. Those incidents represent a total of 68 breaches.

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

Code Chapter	Number of breaches
25 Limiting liability under the guarantee	2
26 What we will tell and give you	76
27 Signing your guarantee	16
28 Withdrawing or ending your guarantee	26
29 Enforcing our rights under the guarantee	0
Total	**120**

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 and
- failure to end guarantees.

Banks reported that most of the incidents 60% were the result of human error and banks identified Part 7 incidents in 40% of cases through line 1 monitoring activities.

Banks reported 102 breaches overall of Part 7 of the Code for the last reporting period. This is an 18% increase.

The BCCC is planning to follow up on the Guarantees Inquiry and would like to see improvements in this area and a reduction of Part 7 breaches in future reports.

Part 8 – Managing your account

Part 8 of the Code (Chapters 30 to 38) largely covers obligations about day to day transactional banking services.

Banks reported 1,299 breaches of Part 8 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	19
31 Statements we will send you	46
32 Cost of transaction service fees	17
33 Managing a credit card	41
34 Direct debits and recurring payments	417

35 Joint Accounts	38
36 Closing any of your banking services	593
37 Your right to copies of certain documents	49
38 When we change our arrangements with you	79
Total	**1,299**

Banks reported a wide range of incidents as breaches under Part 8 and 133,934 customers were affected by these breaches.

Chapter 34 - *Direct debits and recurring payments* related incidents is no longer the category with the highest number of reported breaches in Part 8. Taking its place is Chapter 36 - *Closing any of your banking services*, with 593 breaches, linked predominantly to human error, deficiency in process and procedure, and system error.

The BCCC is pleased to see a reduction in Chapter 34 breaches and encourages banks to continue working on reducing these numbers.

The recent BCCC compliance update: cancellation of direct debits report, showed an improvement on previous BCCC mystery shopping exercises, with 71% of interactions indicating a bank would comply compared to the 2018 compliance rate of 44%. While increases in some bank's individual compliance rates are positive, when compared to historically low rates, a result of 71% is still a significant cause for concern. Further work is required by banks to improve compliance.

Part 9 – When things go wrong

Part 9 of the Code (Chapters 39-45) contains obligations on banks to assist customers experiencing financial difficulty. These provisions relate to timeframes for dealing with requests for financial difficulty assistance, communications with customers, and a commitment to work with and help customers in financial difficulty. Part 9 also contains provisions regarding deceased estates, debt collection and the sale of debts.

Banks reported 4,152 breaches overall of Part 9 of the Code. This represents a 6% decrease from the previous six month reporting period.

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

Code Chapter	Number of breaches	
	Jul–Dec 2020	Jan-Jun 2021
39 Contact us if you are experiencing financial difficulty	303	712
40 We may contact you if you are experiencing financial difficulty	24	19
41 We will try to help you if you are experiencing financial difficulty	1,092	1,142
42 When you are in default	59	68

43 When we are recovering a debt	2,636	1,915
44 Combining your accounts	2	5
45 Helping with deceased estates	318	291
Total	**4,434**	**4,152**

Breaches of Part 9 obligations affected 45,871 customers.

While the decrease in number of breaches from the previous period is encouraging, the total number of customers affected is of concern particularly during a period (COVID-19) where many customers faced financial difficulty.

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
- deceased Estate delays and errors

One Major Bank reported an incident where a system error caused accounts to remain in the hardship system despite the COVID-19 package having ended, impacting 11,859 customers.

The same Major Bank reported an incident where the bank repossessed the asset, a customer's motor vehicle, prior to providing the customer with notification of financial hardship request decline.

Banks reported that 75% of the incidents under Part 9 were the result of human error, with 53% identified and reported by staff.

Part 10 – Resolving your complaint

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

Banks reported 1,434 breaches of Part 10 of the Code for January to June 2021 – a 12% decrease when compared to the 1,629 breaches for the last six-month period. It is encouraging to see an overall decrease in breaches of Part 10. The BCCC hopes that this is an indication that the decrease in reported breaches is a result of banks improving their communication with customers when handling complaints.

Overall the data indicates no large scale systemic failings regarding complaints handling during the reporting period. Banks provided details of 139 incidents that affected 888 customers in total. Where banks provided further details of the incidents, most breaches related mainly to poor communication by banks. Examples include failure to issue final resolution letters to complaints, failure to advise customers that more time is required at the 21-day mark, failure to

provide the name and contact details of the complaint handler and in some instances, failure to register customers' complaints.

Banks reported that most of the incidents (89%) were the result, at least in part, of human error. Consequently, banks reported that they corrected breaches predominantly through staff training, coaching or feedback (76% of incidents).
To remediate these breaches banks most often logged and managed a complaint and communicated with the customer or complainant.

Banks identified Part 10 incidents following line 1 monitoring activities 28% of the time. Staff self-reported the incidents in 51% 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 is focussing 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 is currently in the process of developing its compliance priorities for 2022 – 23, following its wider website stakeholder consultation commenced late last year and will publish this in due course.

The BCCC's Operating Procedures 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. This model is commonly used by subscribing banks and refers to the three "lines" within a business unit responsible for addressing compliance risk. While the model is applied in different ways by banks, generally it features the:

- first line – business units which own the compliance risks and have day-to-day responsibility for breach prevention and compliance monitoring
- second line – the specialist function that develops risk management policies, systems and processes, and
- third line – internal audit with responsibility for reviewing the effectiveness of the compliance framework and independently reporting to the Board.[6]

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

BCCC Contact Details

Website:	bankingcode.org.au
Email:	info@codecompliance.org.au
Postal Address:	PO BOX 14240 Melbourne VIC 8001

BCCC
Banking Code
Compliance Committee