BCCC
Banking Code
Compliance Committee

Banks' compliance with the Banking Code of Practice

January – June 2020

April 2021

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 January to June 2020. The report also includes data for the full 2019–20 reporting period.

This report represents the first opportunity for the BCCC to provide compliance data for the first year of operation of the Banking Code. It is also the first time the BCCC has received detailed information on banks' whole-of-business monitoring methods and systems for several key Code obligations.

The BCCC was mindful of the impact of the COVID-19 on banks' operations throughout 2020 and in May 2020 granted subscribers an extension to respond to the Banking Code Compliance Statement to ensure banks could focus on supporting customers during the pandemic.[1] As we publish this report, the BCCC has already commenced analysis of banks' data for the next period – June to December 2020 – and will report on this data in due course.

An increase in breaches

Banks reported 19,766 Code breaches for the six-month period. Combined with the 20,863 breaches for the previous reporting period, this amounts to over 40,000 breaches of the Code for the year – July 2019 to June 2020. This represents a 160% increase in the number of breaches reported when compared to 15,597 for the 2018–19 period.

While a small percentage of this increase can be attributed to the additional Code obligations that came into effect in 2019 and six new subscribers, banks have explained that the main reason for there being so many more breaches is a result of increased awareness and monitoring of Code compliance, and improvements to risk culture.

The BCCC has for many years viewed increased breach reporting as a positive development, and commended banks for their efforts to identify problems and fix them. It appears that Code compliance is more and more becoming a central part of banks' overall compliance and risk management systems, as well as becoming embedded in staff communications and training.

However, there will come a time where the BCCC, and the broader community, will expect banks to have gained sufficient insight from this breach data to prevent compliance incidents from happening in the first place. The data indicates that in some areas, such as privacy and

[1] Further information about the Banking Code Compliance Statement is provided on Page 6 of this report and in the BCCC's Guidance Note 1: Breach Identification and Reporting, published in September 2019

confidentiality, large numbers of breaches have been reported for many years and the BCCC will expect to see a significant decrease in the number of reported breaches. For other Code obligations, for example taking extra care with customers experiencing vulnerable circumstances, breaches may continue to increase as banks continue to improve compliance monitoring practices and strengthen staff awareness of their commitments.

The BCCC cannot predict when the tipping point will come, and the total number of breaches will start to decrease, but when it does it will be a welcome demonstration that banks are meeting the high ethical standards set out in the Code. The BCCC recently published its Report on *Building Organisational Capability*, which provides banks with guidance as they shift from building robust systems to detect breaches, to building more robust systems to prevent breaches. [2]

What are banks self-reporting?

As with the BCCC's previous compliance reports, we have analysed and reported on breaches of the 10 'Parts' of the Code and provided an analysis of trends and the nature of breaches of Chapters and obligations within these Parts. Banks reported notable increases in the number of breaches under Part 4 *Inclusive and accessible banking*, which includes the obligation to take extra care when dealing with a customer experiencing vulnerable circumstances, and Part 6 *Lending to small business*. However, Part 2 of the Code continues to account for the largest number of breaches.

Table 1. Number of Code breaches, By 'Part'

Code 'Part'	Jan to Jun 2020	Jul to Dec 2019	% change
Part 2 Your banking relationship	8,519	10,957	Down 22%
Part 9 When things go wrong	3,662	3,949	Down 7%
Part 5 When you apply for a loan	2,557	2,456	Up 4%
Part 3 Opening an account and using our banking services	2,019	1,461	Up 38%
Part 10 Resolving your complaint	1,206	1,248	Down 3%
Part 8 Managing your account	821	447	Up 84%
Part 4 Inclusive and accessible banking	504	154	Up 227%
Part 6 Lending to small business	316	107	Up 195%
Part 7 Guaranteeing a loan	146	68	Up 115%
Part 1 How the Code works	16	15	Up 1%
Code Transition		1	-
Total	**19,766**	**20,863**	**Down 5%**

[2] BCCC Report - Building Organisational Capability: How banks can improve compliance with the Banking Code of Practice and deliver better customer outcomes, February 2021

COVID-19 related breaches

The BCCC would be remiss if it did not address the impact of the COVID-19 pandemic upon banks' compliance with the Code. For this report we have assessed breach incidents that were reported as, or appear to be, a direct result of conditions created by the pandemic.

Some banks reported an increased workload and resourcing issues as a direct cause of some breaches. Other breaches point to ongoing work that may need to be addressed by banks, such as privacy concerns with staff working from home.

However, COVID-19 does not appear to have significantly affected banks' ability to comply with the Code when it is considered in the context of the overall impact of the pandemic on the Australian economy, customers' lives and livelihoods and banks' business operations.

Scams and fraud

While the Code does not contain any specific provisions related to scams and fraud, banks play a crucial role in protecting customers from the predatory behaviour of scammers and criminals.

Banks reported a number of significant and upsetting scam and fraud events that were often recorded as breaches of obligations relating to privacy and confidentiality provisions, taking extra care when dealing with customers experiencing vulnerable circumstances, or staff training and fair and reasonable conduct.

Our main intention in highlighting these incidents in this report is to indicate where banks' real-time monitoring and systems controls could be improved to protect customers at risk.

Data consistency and quality

As the BCCC confirmed in its previous compliance data report, there can be a wide variance between banks in terms of the quality and consistency of the data provided in their responses, and we remain concerned that if banks apply different standards in monitoring, detection and reporting of Code breaches it makes the data less reliable and reduces transparency.

The BCCC is engaging with the Australian Banking Association (ABA) as it works with its member banks to understand the issues that lead to data quality and consistency issues. The BCCC welcomes this work by the ABA and anticipates that it will lead to more streamlined and reliable breach data reporting in the future.

Ian Govey AM

Independent Chairperson

Banking Code Compliance Committee

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. Nineteen banks subscribe to the Code.

The BCCC

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 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.

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.

Previously, under the 2013 Code of Banking Practice, banks reported which obligation had been breached and then described what occurred. The BCCC now 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.

The Report

This report mostly summarises banks' Code breach data for the reporting period of January to June 2020, but in some cases covers the whole 12-month period – July 2019 to June 2020. The BCCC has referred to the first six months of 2019–20 (July to December 2019) as 'Period 1' and the latter six months (January to June 2020) as 'Period 2' throughout the report.

In other cases, we have also included longer term trend data for previous reporting periods covering the 2013 version of the Code. Readers should use caution when making direct comparisons between different reporting periods because the number of banks subscribing to the Code and the Code obligations have changed over time.

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 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 (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, one bank reported 2,917 total breaches for Period 2 and further details of 366 incidents which accounted for 2,140 breaches. These 366 incidents affected 1.3 million customers and a financial impact of more than $50 million.

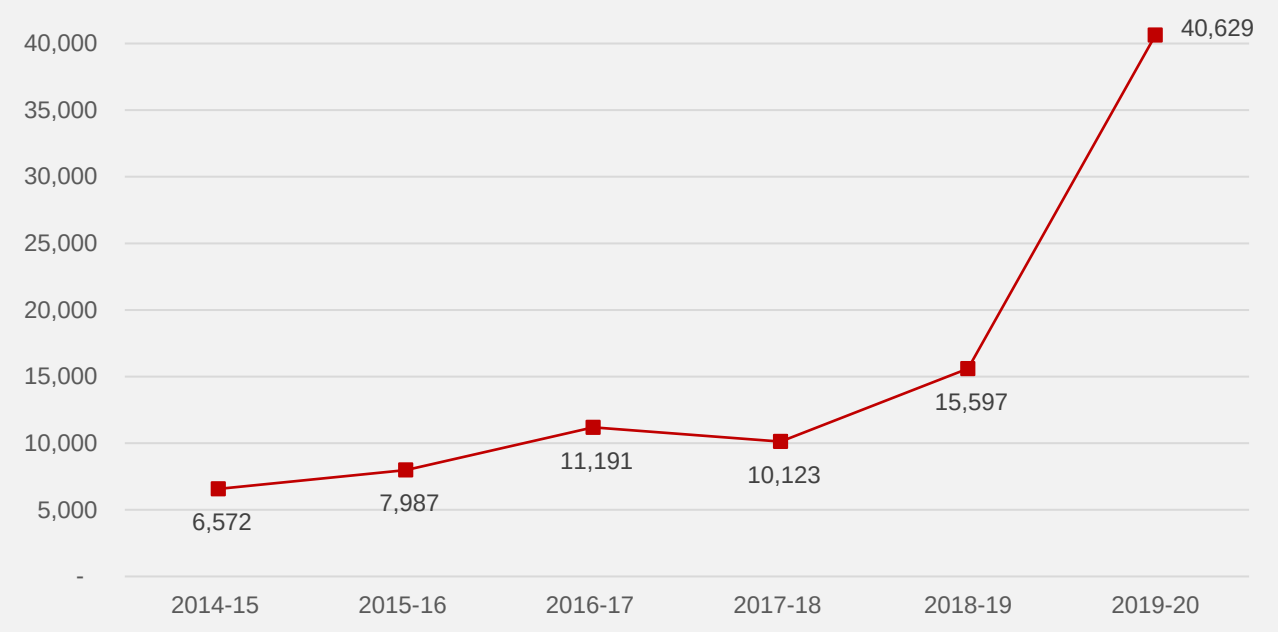
The BCCC has also included de-identified examples based on individual breaches where the incident is of particular interest or concern.

Summary of breaches overall

The 12 months from July 2019 to June 2020

The 19 banks that subscribe to the Code reported 40,629 breaches of the Code for the 12 months July 2019 – June 2020. This represents a 160% increase on the 15,597 breaches reported for the 2018–19 period.

Chart 1. Total number of Code breaches, 2014–15 to 2019–20[3]



Eleven of the 13 banks that subscribed to the 2013 version of the Code reported an increased number of breaches – with the four major banks' breaches increasing between 99% and 646%.

The reasons provided by banks 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
- the addition of new breach obligations in the Code and an increased focus on identifying breaches of the 'fair, reasonable and ethical behaviour' obligations
- increased focus on identifying more than one Code breach per incident (in accordance with the BCCC's guidance) which led to an increase in the number of breaches reported without an equivalent increase in the number of compliance incidents, and

[3] Data for 2014–15 to 2018–19 includes the 13 subscribers to the 2013 Code. 2019–20 data covers the 19 subscribers to the current Banking Code. The six new subscribers account for 2% of the total number of breaches for 2019–20.

- greater diligence and additional resources to ensure breaches are identified, recorded and appropriately reported to the BCCC.

Another factor that can affect the number of breaches reported is a bank's assessment of whether a particular type of incident consists of one breach that affects many customers, or whether many incidents are a product of one systemic breach. Banks' assessment of these issues will likely form part of the ongoing work to improve the consistency of approach between the banks.

Table 2 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 2019–20, and one of these major banks reported more than 40% of the 40,629 total for this period. Banks D, E, G, L, and O did not subscribe to the 2013 version of the Code.

Table 2. Total number of Code breaches, By Bank, 2014–15 to 2019–20

Bank	2014–15	2015–16	2016–17	2017–18	2018–19	2019–20	*2019–20*	
							Jul–Dec 19	*Jan–Jun 20*
Major Bank 1	3,592	4,832	8,064	5,848	8,539	16,958	*8,811*	*8,147*
Major Bank 2	309	210	320	1,060	1,212	9,045	*6,128*	*2,917*
Major Bank 3	365	912	800	718	2,331	5,600	*2,140*	*3,460*
Major Bank 4	390	450	420	455	1,108	4,586	*1,660*	*2,926*
Bank A	31	82	240	283	377	1,350	*506*	*844*
Bank B	21	152	168	447	639	720	*428*	*292*
Bank C	1,095	975	649	875	867	608	*293*	*315*
Bank D						366	*249*	*117*
Bank E						296	*161*	*135*
Bank F	9	31	30	39	80	250	*124*	*126*
Bank G						197	*91*	*106*
Bank H	131	177	258	145	134	194	*106*	*88*
Bank I	17	24	31	44	89	125	*32*	*93*
Bank J	465	100	146	151	127	116	*57*	*59*
Bank K	147	41	62	58	79	98	*47*	*51*
Bank L						57	*16*	*41*
Bank M		1	3		15	30	*11*	*19*
Bank N						29	*2*	*27*
Bank O						4	*1*	*3*
Total	**6,572**	**7,987**	**11,191**	**10,123**	**15,597**	**40,629**	***20,863***	***19,766***

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

Table 3. Number of breaches, by Code 'Part'

Code 'Part'	Number of breaches (12 months)	Period 1 (Jul–Dec 2019)	Period 2 (Jan–Jun 2020)	% of total (12 months)
Part 2 Your banking relationship	19,476	10,957	8,519	48%
Part 9 When things go wrong	7,611	3,949	3,662	19%
Part 5 When you apply for a loan	5,013	2,456	2,557	12%
Part 3 Opening an account and using our banking services	3,480	1,461	2,019	9%
Part 10 Resolving your complaint	2,454	1,248	1,206	6%
Part 8 Managing your account	1,268	447	821	3%
Part 4 Inclusive and accessible banking	658	154	504	2%
Part 6 Lending to Small Business	384	68	316	<1%
Part 7 Guaranteeing a loan	253	107	146	<1%
Part 1 How the Code works	31	15	16	<1%
Transition Period	1	1	0	<1%
Total	**40,629**	**20,863**	**19,766**	

The COVID-19 pandemic and its effects on the banking industry and the broader economy are discussed in more detail elsewhere in this report and most of Period 2 (Jan–Jun 2020) occurred after the pandemic started to impact the Australian community.

Banks have reported considerable increases in requests for financial difficulty assistance and loan deferrals and in many cases a significant proportion of staff were re-allocated to relevant customer support teams.

One might expect to see that breaches of Code obligations related to Part 9 (*When things go wrong* (debt recovery and financial difficulty)) and Part 10 (*Resolving your complaint*) would increase in the second half of the 12-month reporting period. However, overall this was not the case. Banks reported broadly consistent numbers of breaches in these areas over both Period 1 and 2. Nevertheless, one major bank reported a significant increase in debt recovery breaches due to the increased volume of calls and associated monitoring during Period 2, and another major bank reported significantly less financial difficulty breaches. Several banks reported that Code monitoring activities for financial difficulty obligations were reduced or paused for some of Period 2 and the number of breaches identified may have been affected as a result.

There was a significant increase in reported breaches of Part 4 of the Code (*Inclusive and accessible banking*) from Period 1 (154) to Period 2 (504). The major increase within this Part was under Chapter 14 – 'taking extra care with customers who may be vulnerable'.

Breaches for January to June 2020 (Period 2)

In accordance with the BCCC's reporting instructions (see p. 6), banks provided further information about the nature, cause, impact and correction of 2,555 incidents for Period 2, constituting 7,507 breaches – 38% 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 (70%) were caused by human error alone, and a further 5% caused by human error plus another factor. 11% involved a control, training or resourcing failure (including process deficiencies) and 10% involved a system error. Banks attributed business disruption due to COVID-19 as the explicit cause of only 13 incidents (or 0.5% of the total).

The BCCC has, for several years, encouraged banks to both look beyond human error alone to identify underlying causes, including those related to systems, processes, training and culture, and to improve organisational capability to support staff to comply.

As part of its analysis and preparation of this report, the BCCC has examined breach incident reports in detail. This examination indicates that some breaches attributed to human error could and should have been avoided, had better systems and processes been in place. We will provide feedback to individual subscribers to which this applies, to help improve their compliance in the future.

More broadly, the BCCC's recent publication of its *Building Organisational Capability* Report identifies key capability areas and recommendations for better practice in the following areas to improve Code compliance:

- Communication strategy
- Learning and development
- Systems, processes and technology
- Culture
- Enhancing capability through robust compliance frameworks

The impact of the breaches

Overall the sample of incidents reported for January to June 2020 affected more than 3.5 million customers, with a total financial impact of over $123 million.

There are difficulties with reporting on the financial impact of breaches and the BCCC currently does not consider the dollar amount to be an accurate reflection of overall financial impact of non-compliance with the Code.

This is because of the wide variance across incident reports in how financial impact is reported. The BCCC plans to review its guidance and data requirements for financial impact reporting to improve accuracy and consistency.

Despite these data integrity issues, the BCCC considers it is important to report on the data it has received to highlight the impacts of failures to comply with the Code, even where there may be data consistency challenges.

How the breaches were corrected

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 (15%)
- review staff performance or taken disciplinary action (8%).
- implemented a system fix (7%), and
- enhance monitoring or controls (5%).

Bank actions to prevent recurrence were still under review at the time of reporting for 8% of incidents. Banks did not provide details of efforts to prevent recurrence for 7% of incidents. Banks reported that they did not take actions to prevent recurrence or no action was required for approximately one percent of incidents.[4]

Banks still rely, to a significant degree, on staff training and feedback as a corrective action to most breaches. We anticipate that in future banks will fully integrate the findings and recommendations within the *Building Organisational Capability* Report and focus on building more robust systems and processes to prevent breaches reoccurring.

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 (30% of incidents)
- provided financial remediation, such as a refund, debt waiver, compensation or goodwill payment (23%)
- communicated or corresponded with the customer (16%)
- apologised to the customer (10%)
- logged, managed or resolved a complaint (3%), and
- referred customers for financial difficulty assistance (<1%).

Banks reported there was no customer remediation provided or customer remediation was not required for 9% of incidents. For 13% 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 5% of incidents or confirm that these breaches were still under investigation. The BCCC will continue to provide feedback to the banks involved to ensure that complete information is provided in future reporting.

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

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.[5]

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.

31% of incidents were identified as a result of customer complaints, queries or feedback. The other most prominent methods of breach identification were self-identification by staff members (26%) and via line 1 quality assurance activities including call monitoring and system monitoring (25%). A further 9% of incidents were identified by line 2 or internal reviews, 4% via external parties or events and 3% from Australian Financial Complaints Authority (AFCA) decisions.

Summary of banks' monitoring activities

Once a year for the relevant reporting period, in this case July 2019 to June 2020, the BCCC requires banks to provide information on their approach to monitoring compliance with the Code, in order to gain insight into their monitoring and oversight activities.

The BCCC requested information regarding the monitoring of the following five obligations:

- responsible lending
- debt recovery
- complaints handling (or Internal dispute resolution (IDR))
- financial difficulty, and
- guarantees.

Overall the BCCC found the banks' monitoring frameworks to be well structured and holistic in nature with banks employing a range of methods to identify instances of non-compliance with their Code obligations, primarily through quality assurance reviews, call monitoring and control testing. These are largely aligned with the BCCC's expectations in relation to Code monitoring and breach identification.[6]

[5] 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*, April 2018

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

In contrast to the general theme around method of incident identification for Code obligations as a whole, line 1 monitoring was the predominant method of identification for the five obligations under review – accounting for 38%. The proportion of incidents identified through line 1 monitoring across all Code obligations was 26% for the full year.

Compliance monitoring of responsible lending obligations appeared to be the most comprehensive and robust, with most banks conducting monitoring activities across different stages of the application process through more than one monitoring method.

Through its review of the banks' responses, the BCCC also observed several examples of good monitoring practices undertaken by the industry. These are shared later in this report.

Nevertheless, in general banks did not provide information about ongoing testing of the automated systems relied on to meet their compliance obligations such as credit decision engines, credit scorecards, IDR case management systems or the collections dialer systems. Only one bank (a major bank) reported undertaking regular system testing for all areas under review.

Additionally, some banks either did not conduct any call monitoring or conducted minimal monitoring of their customer interaction channels.

One of the smaller banks reported undertaking no monitoring or oversight of its compliance with debt recovery, financial difficulty and guarantees obligations for the period under review. The bank did not report any breaches of the relevant obligations. The BCCC expects all banks to have continuous oversight over their Code obligations as part of their commitment to customers, and while the BCCC will follow up with the bank, it has confirmed it will allocate a dedicated resource for the monitoring function moving forward.

Due to the impact of COVID-19 during 2020, some banks reported temporarily scaling back their monitoring activities, mainly to reallocate resources to their frontline teams or because of access limitations as part of working from home. The BCCC understands the unique challenges posed by the pandemic and banks need to be agile in the face of these issues. Nevertheless, we strongly encourage banks to maintain robust oversight of their Code compliance obligations where possible to ensure customers are being treated in a fair, reasonable and ethical manner.

COVID-19 impacts on Code compliance

There is little need for the BCCC to comment in detail on the impacts of COVID-19 on the Australian economy, other than to say it has and will continue to have a substantial effect on the way Australians work and do business.

Banks temporarily closed or reduced contact hours for their branches and thousands of employees were re-allocated from branches and other areas to deal specifically with COVID-related financial difficulty and deferral matters. Hundreds of thousands of customers sought COVID-related deferrals of business, personal and home loans at the height of the crisis.

Based on the breach data provided by banks for the period January to June 2020 and our engagement with a range of stakeholders over the last 12 months, the BCCC is of the opinion that banks responded well overall to the operational challenges they faced.

COVID Special Note amendment to the Code

Circumstances created by COVID-19 may affect banks internal resources and capacity, and as a result the ABA sought the Australian Securities and Investments Commission's (ASIC) 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 consequently did not apply to banks for the reporting period covered by this report.

BCCC approach to COVID-specific breaches

The BCCC considers that that COVID related and specific breaches were worthy of deeper examination and commentary.

A number of breaches were reported by several banks as being caused by COVID-specific workload issues or were the result of staff working from home due to the pandemic, as well as breaches of Code-required timelines for correspondence and responses.

The BCCC has classified several hundred breaches as COVID-specific. We recorded a total of 687 Code breaches related to or caused by the pandemic. One major bank reported the majority of these breaches, with 544 breaches relating to two types of incidents: complaints handling delays; and failing to meet requirements to assess hardship applications within 21 days as a result of an increase in volumes due to COVID. These breaches affected 544 customers and each case was determined to be a breach of the Code.

Other banks reported breaches which impacted many hundreds or thousands of customers but categorised these incidents as single systemic breaches. Overall, more than 50,000 customers were affected by COVID-related breaches of the Code.

The nature of the incidents

The nature of the incidents banks reported include:

- incorrect information being provided to customers enquiring about COVID relief/deferral options, including providing incorrect information on websites
- deferrals being incorrectly actioned, including credit cards being suspended due to non-payment
- deferrals placed on accounts without the customer requesting the bank to do so
- 'working from home' issues such as staff using personal email accounts for confidential documents and information
- delays in responding to financial difficulty requests and complaints, and
- a range of other transactional and processing issues.

The pandemic will continue to impact the economy and the BCCC will monitor COVID-specific events for the foreseeable future. The BCCC has also required banks to provide information for the 2020–21 period regarding any incidents that would have been a breach of the Code if not for the exemptions in place under the Code's Special Note.

Scam and fraud related breaches

The Australian Competition & Consumer Commission's (ACCC) Scamwatch statistics indicate that Australians lost more money to scams in 2020 than in 2019 and the ACCC has issued a number of warnings that some types of scam are on the rise during the pandemic.

The Australian Competition and Consumer Commission's Scamwatch website lists some of the more common scams, including:

- 'Dating and Romance' scams which take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions.
- 'Tax Office' scams, where victims are advised of a non-existent tax or other debt that must be paid immediately.
- 'Unexpected money' scams which may ask for bank account details to 'help them transfer the money' and use this information to later steal funds, or to transfer funds to 'help release or transfer the money out of the country' through customers' bank accounts.
- 'Remote access scams' where a scammer will impersonate someone calling from a major company, which may include a bank, and may request access to a computer or account.
- 'Phishing' and identity theft scams, where scammers use various methods to steal personal information and once obtained, use people's identity to commit fraudulent activities such as using credit cards or opening bank accounts.

Scammers are also using the COVID-19 pandemic to take advantage of people across Australia through vaccination, superannuation, financial assistance and other scams targeting individuals and businesses.

BCCC approach to assessing scam and fraud related Code breaches

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

We identified more than 70 breaches of this kind and while this is not an unduly large number, the incidents were of a serious nature. Many of the incidents occurred because of failures in systems and procedures, or staff failing to follow correct procedures.

Examples of incidents of scams and fraud include:

- withdrawal of funds in-branch using stolen cards or other identification documents
- family members accessing a vulnerable customer's funds without authority
- phone and internet transfers where a person impersonates the customer
- employees not following process and procedure in adequately asking the relevant questions to a customer to understand the purpose of withdrawals
- employees not conducting the necessary checks and reviews to intervene and assist a customer in potentially avoiding being scammed, and
- employees not completing identification processes correctly, resulting in fraudulent withdrawals from accounts.

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

In one particularly concerning case, a bank allowed transfers to an overseas investment scam which had previously been the subject of ASIC advice to all Australian financial institutions.

The impact of the incidents

Of the incidents the BCCC classified as scam or fraud-related, 90 customers were impacted, with a financial impact of over $2.8 million.

Some of the most serious financial losses were:

- a criminal withdrew over $250,000 in branch without the customer's knowledge
- three cases where victims transferred over $100,000 to scammers
- one case of a staff member stealing $167,000 from a vulnerable customer over a period of months, and
- a number of cases of 'phone porting', a form of identity theft, causing losses to customers of over $100,000.

These figures make clear that fraud and scams have an enormous impact on individual customers.

The BCCC encourages 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.

The BCCC is currently conducting an inquiry into banks' compliance with the obligations under Part 4 of the Code which includes the requirements to take extra care with customers who may be vulnerable, including those who may be the victims of scams.

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

Part 2 of the Code contains Chapters 3 to 7. Banks reported a total of 8,519 breaches of Part 2, comprising:

- Chapter 3 – Our compliance with this code – 8 breaches
- Chapter 4 – Trained and competent staff – 4,631
- Chapter 5 – Protecting Confidentiality – 3,869
- Chapter 6 – Compliance with laws – 10
- Chapter 7 – Closing a branch – 1

Banks provided further information about the nature, cause, impact and correction of 1,385 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.

Banks will often be required to conduct a subjective assessment of incidents to classify whether conduct is a breach of these obligations. If an incident results in a breach of any other Code provision, that incident could also be a breach of Chapter 4 provisions.

For this reason and because, in some cases, Chapter 4 appears to be used as a 'catch-all' when classifying some breach incidents, 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 on elsewhere in this report, banks tend to:

- blame human error for breaches where better systems (IT and otherwise) may have prevented staff from making the error, and
- over-rely on staff training and feedback as a means 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 3,869 breaches reported for Period 2, although there has been a 34% decrease since Period 1.

While banks reported that the majority of privacy and confidentiality breaches did not have a financial impact on customers, many concerning Chapter 5 breaches resulted in significant financial and other consequences for customers. These include:

- insufficient identification checks resulting in fraudulent activities, and
- sending correspondence about a new home loan to customer's previous address, which may have the customer at risk because they are a victim of domestic violence.

Other common privacy and confidentiality incidents include:

- providing information to the wrong party, and
- staff emailing confidential or a customers' personal information to their personal email accounts.

More than 70% of privacy and confidentiality incidents were classified as being caused by human error and staff training and feedback was listed as the corrective action for more than 60% of them. The BCCC considers that 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 2,019 breaches of Part 3 obligations in total and further details about 371 incidents (or 626 breaches). The breaches were generally related to banks providing incorrect or misleading information or advice to customers, and incorrect fees and charges.

Banks reported that most of the incidents (53%) were the result of human error. 20% were the result of a deficient process or procedure. Banks identified Part 3 incidents following complaints from the customer in 32% of cases, followed by self-identified or reported by staff member (27%).

134,000 customers (with a financial impact of $1,000,000) were affected by a single breach reported by one bank where the bank sent incorrect information to customers advising them their balance transfer was about to expire.

Banks provided financial remediation to customers for 29% of these Part 3 breach incidents. Banks' corrective actions to prevent further breaches were predominantly through staff training, coaching or feedback (45%).

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 vulnerable.

The BCCC considers Part 4 to be a priority for its monitoring activities and is currently conducting an inquiry into banks' compliance with these provisions.

Banks reported 504 breaches overall of Part 4 of the Code for Period 2 – January to June 2020.

Increase in reported breaches

Seven banks did not report any breaches of obligations under Part 4 in Period 1 and the BCCC stated that it understood that many of the obligations under Part 4 were new requirements and in some cases, banks would be continuing to develop policies, processes and staff training to meet these requirements.

While there has been a considerable increase in the total number of breaches reported in Period 2, the overall number of banks reporting breaches of Part 4 was consistent with Period 1. Three of the four major banks reported increases, for two of them, significant increases.

The increase in these breaches can be attributed in part to the impacts of the pandemic and bushfires, but also to increased monitoring and awareness on this Part of the Code. For example, one major bank noted:

> *"…compliance programs have supported an increased focus on key clauses of the code. There has been a specific focus and work in the identification of breaches relating to vulnerable customers over the last 12 months and there is heightened awareness across the group, resulting in an increase in identified breaches across these chapters."*

And another stated:

> *"…establishment of training across frontline channels to identify vulnerable customers made it easier for staff to recognise errors and record them as incidents. Also, an increased focus on targeted QA monitoring and usage of speech analytics to detect customers experiencing vulnerability and register complaints."*

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

Code Chapter	Number of breaches Period 1 Jun–Dec 19	Number of breaches Period 2 Jan–Jun 20	Number of breaches 12 months
13 Being inclusive and accessible	25	45	70
14 Taking extra care with vulnerable customers	101	347	448
15 Banking services for people with a low income	18	101	119
16 Basic accounts or low or no fee accounts	10	11	21
Total	**154**	**504**	**658**

Banks provided further information about the nature, cause, impact and correction of 49 incidents related to Part 4 for Period 2.

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

- failure to identify or take extra care with customers who may be vulnerable
- 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 or a Financial Management Order.

Banks reported that most of the incidents (65%) were the result of human error and 54% of Part 4 incidents were identified following complaints from the customer.

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.

Lending data

The BCCC required banks to provide details about the number of applications for credit where the bank's assessment was completed during the reporting period to provide further context to the compliance data banks are reporting. During the 12-month 2019–20 period banks assessed more than 4.6 million applications for credit.

Table 5: Breakdown of credit applications, By product type, 2019–20

Product type	Number of applications (individual customers)	Number of applications (small business customers)	Total number of applications
Credit cards	1,513,675	19,170	1,466,745
Home loan – owner occupier	935,828	13,875	937,837
Unsecured loan (fixed term)	827,565	15,446	840,239
Secured personal loan (for example, car loan)	322,170	86,844	409,014
Home loan – investor	316,813	9,080	319,922
Credit card limit increases	275,252	3,407	274,655
Secured business loan	116	199,675	199,791
Other	83,145	59,728	142,905
Overdrafts	54,339	13,315	67,654
Total	**4,328,903**	**420,540**	**4,658,762**

Breach data

Banks reported 2,557 breaches overall of Part 5 of the Code for the reporting period between January – June 2020 (Period 2).

Overall, for the 12-month period, banks reported 5,013 breaches of Part 5 of the Code.

Nearly all Part 5 breaches are of Chapter 17, with breaches of the other chapters (covering the selling of consumer credit insurance and lenders' mortgage insurance) being nominal.

Chapter 17 – A responsible approach to lending

Chapter 17, *A Responsible approach to lending*, was the Chapter with the third highest number of breaches for Periods 1 and 2.

One major bank reported 40% of all Chapter 17 breaches for Period 2. Six banks did not report any breaches of Part 5 or Chapter 17.

Banks provided further information about the nature, cause, impact and correction of 256 incidents related to breaches of 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
- misleading or incorrect information or advice provided to customer.

One bank reported an incident where a couple were approved for a $30,000 personal loan to buy a car. Once this loan was reviewed it was found that it was unsuitable given the age of the customers. The customers were aged 77 and 88 at the time of the application for the five-year unsecured personal loan. The customers had no other assets to offset the debt and were reliant on their pension to make the repayments. The older customer subsequently went into permanent care due to dementia. Further inquiries found that the customers had a number of other credit cards that did not appear to have been disclosed at the application stage. While the bank could not discriminate against customers because of their age, the bank confirmed it should have made further inquiries given the customers' age and the potential for them to be experiencing vulnerability.

Banks reported that most of the incidents (68%) were the result of human error. Banks identified 35% of Chapter 17 incidents by line 1 monitoring activities and 23% were identified as a result of customer complaints.

Banks' approach to compliance monitoring of responsible lending obligations

Banks' frameworks for monitoring the responsible lending obligations (RLO's) can be considered the most formally structured and well embedded across all the key obligations reviewed by the BCCC. There also appears to be considerable rigour around their monitoring and oversight practices with banks reviewing the end to end credit application process through quality assurance (QA) of lending files, call monitoring and hindsight reviews at the pre and post drawdown stages. Although their approaches varied, mainly owing to their size and nature of business, all banks reported having an active monitoring programme in place with more than one method being applied to proactively identify breaches.

For the 12-month period (Periods 1 and 2) banks reported identifying 42% of the incidents through their line and 1 and 2 functions with most banks classifying 'hindsight' reviews as line 2 monitoring. Further to this, the bank that disclosed the highest number of RLO breaches for the year, reported identifying 68% of these through its line 1 and 2 monitoring functions.

A substantial portion of incidents of non-compliance with RLO's continue to be identified through customer complaints and feedback. According to the data 25% of incidents for the full year were identified through this channel.

Banks reported conducting reviews at pre and post drawdown stages, with almost all banks reporting some degree of reliance on automated systems for credit assessment or the overall approval process. Some banks reported undertaking assurance reviews of credit applications across different stages and teams to enable a larger population of the applications to be tested based on varying criteria. For example, one of the banks conducts a hindsight review on 10% of fully settled applications through random sampling, while another business unit conducts a risk-based review of a sample of these applications.

Also, two of the banks stated they made phone contact with the customers once their applications were approved to understand if there had been any material changes to their circumstances owing to the impact of COVID-19 and to discuss the next steps accordingly.

Banks generally had formal and well-defined channels to report monitoring outcomes to risk committees and senior management including escalation of issues and emerging trends.

As part of their COVID response several banks also reported conducting targeted reviews of the impacted credit facilities.

Nevertheless, six banks either did not undertake any call monitoring specific to credit applications or did not report it as part of their response. Also, a small number of banks advised undertaking application reviews at pre-drawdown stage as part of the assessment only, which could be considered a part of the process rather than independent monitoring of the application.

One of the banks reported conducting monitoring only on applications it considered 'high risk' through its monitoring framework, reviewing 10% of all lenders each month with the hindsight process focused only on the judgement aspect of the credit decision. Based on this methodology it is likely that only high-risk applications will be tested with the bank having little or no oversight over the credit quality of the majority of its applications.

The BCCC is also concerned that only 6 of the 19 banks have reported undertaking any ongoing testing of their automated systems used in the credit application process such as credit decisioning engines and scorecards to ensure that they are functioning as designed, at the same time acknowledging that elements of their credit processes are subject to system processing or assessment, mostly at the pre-assessment or credit scoring stages. A few banks reported only testing the automated systems or the embedded rules as part of any changes made to the criteria or the functionality of the system in question.

Examples of good practice initiatives included:

- One bank conducts observations of mobile bankers' non-call interactions with clients as part of the customer interaction monitoring methods.
- Complaints identified on auto finance loans originating through a dealer are part of the selection criteria for quality assessment file selection at one of the banks. Where an RLO breach has been identified details are recorded in a central repository for review by senior management for possible consequence management in line with their third-party management policies.

- The same bank carries out an ‘outlier’ review of its branch staff, where the senior manager selected staff members’ outlier data to undertake investigation on all systems to determine if any RLO breaches or inappropriate sales practices have occurred in the process of customer applications. Any adverse findings would directly affect the staff members’ variable remuneration.
- Similarly, another bank conducts targeted sales monitoring focusing on top performing sales staff to check for any behavioural concerns.
- Qualitative file reviews conducted by the same bank on personal loan and credit card applications originated by branch and mobile banking staff focused on the quality of information captured in the lending application including the product suitability and the joint borrower substantial benefit requirement. The purpose of these reviews is to provide ongoing education to front line bankers.
- Another bank conducted a responsible lending survey across all relevant teams to understand their awareness of the obligations.

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 316 breaches overall of Part 6 of the Code for Period 2.

This is a significant increase on the previous reporting period, where only 68 breaches were reported. In that period only five banks reported breaches, with one major bank reporting 80% of the breaches. The same five banks reported breaches of Part 6 for this period.

One bank reported 254 of Period 2's breaches and noted that the increase is due to improved automated detection of failure to send pre-application disclosure materials along with increased awareness of the Chapter 20 requirements among staff resulting in higher levels of breach self-reporting.

Another major bank reported an increase in Part 6 breaches from 7 to 50. This was reported as one incident related to the provision of external valuation reports to 50 small business customers.

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

Code Chapter	Number of breaches Period 1 Jun–Dec 19	Number of breaches Period 2 Jan–Jun 20	Number of breaches 12 months
20 Helping a small business when it applies for a loan	59	260	319
21 When will we not enforce a loan against a small business?	1	0	1
22 Specific events of non-monetary default	0	1	1
23 When we decide not to extend a loan	2	5	7
24 When we appoint external property valuers, investigative accountant and insolvency practitioners	6	50	56
Total	**68**	**316**	**384**

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

- deficiencies in documentation
- incomplete provision of valuation documents, and
- credit assessments being incomplete or unsatisfactory.

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 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 we will be shortly reporting on a major Inquiry into these obligations that has been underway since 2019.

Banks reported 146 breaches overall of Part 7 of the Code for Period 2.

For the previous 12-month period, from July 2018 to June 2019, banks reported 118 breaches of the guarantees provisions under the 2013 Code.

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

Code Chapter	Number of breaches Period 1 Jun–Dec 19	Number of breaches Period 2 Jan–Jun 20	Number of breaches 12 months
25 Limiting liability under the guarantee	72	5	77
26 What we will tell and give you	25	81	106
27 Signing your guarantee	5	37	42
28 Withdrawing or ending your guarantee	3	22	25
29 Enforcing our rights under the guarantee	2	1	3
Total	**107**	**146**	**253**

Approximately 70% of incidents reported by banks involved incorrect or inaccurate information being provided to guarantor, information not provided to guarantor, or information not provided at appropriate time.

Examples of breaches of guarantee obligations include:

- One bank's inability to provide written notification to guarantors as a result of a change of their loan due to COVID-19 payment deferrals, affecting more than 36,000 customers.
- Another bank did not send copies of arrangement letters, that were sent to customers, to personal guarantors during the COVID-19 crisis period. The bank was arranging to send the letters to the 150 guarantors affected at the time of reporting to the BCCC.

- A bank did not comply with its guarantee obligations under the Code because it gave the guarantee to the borrower's representative for execution. The case went to AFCA and it recommended that the bank waive the complainants' liabilities under the guarantee, amounting to over $250,000.
- Another bank reported an incident that arose as a result of a family dispute. There were three parties to a mortgage over an owner-occupied property, with the third party being a guarantor. The loan was paid out in full and the guarantor requested discharge of the security. The bank followed its process by requiring all parties to the mortgage to sign the discharge. However, the borrowers refused to sign the discharge due to a family dispute. The guarantor referred the matter to AFCA and it found the bank should have discharged the mortgage based on the guarantor's equitable right of redemption. The bank discharged the security and paid $3,000 compensation to the guarantor.

Banks reported that most of the incidents (60%) were the result of human error and banks identified Part 7 incidents in 49% of cases through line 1 monitoring activities.

Banks' approach to compliance monitoring of guarantee obligations

A review of bank responses indicates that monitoring compliance with guarantees obligations is principally undertaken as part of the responsible lending monitoring framework. Only two of the banks reported conducting specific quality assurance monitoring on guarantor loans, while some banks, irrespective of their size, assessed all loan applications with a guarantor manually.

The BCCC acknowledges that smaller banks tend to have lower guarantor loan volumes with some reporting that they accepted guarantees in very limited circumstances. In addition, at least two banks advised that they outsourced their guarantees process or obligations to external parties such as solicitors.

Data provided by the banks indicates that line 1 monitoring identified the highest number of incidents followed by the self-identified category. Together, both accounted for 74% of the incidents identified during the 12-month period under review.

The industry reports widespread use of checklists, templates and peer review checks at different stages of the guarantees process to achieve compliance, mainly with the provision of information and documentation requirements, with more than 81% of incidents of non-compliance identified pertaining to Chapters 26 and 27 of Part 7 for the six-month period ending June 2020.

Some banks had specialist document verification teams or a quality check function at application and settlement stages that used guarantor suitability and document checklists to confirm all relevant requirements prior to forwarding the file to the next stage, while some banks relied on formal peer review checks as part of document verification.

Banks also reported undertaking guarantees-related targeted reviews and audits, including audits conducted as part of the BCCC's Guarantees Inquiry.

However, banks provided little or no insight into their approach to monitoring compliance with the post-approval stage of the guarantees such as withdrawal and enforcement.

The reporting of monitoring outcomes to senior management specific to guarantee outcomes was not conducted or reported by most banks. This can be largely attributed to the combined lending and guarantees obligation monitoring model adopted by the industry.

Examples of good practice initiatives include:

- For one bank that manually assesses all guarantor applications, branch management conducted an additional check on branch and mobile lending staff applications to ascertain if all guarantor documents were held in file and that the 3-day Code requirement had been met. Another aim of this check was help uplift staff competency and provide coaching to create awareness.

- Another bank that only has a small volume of guarantor loans and conducts random sampling as part of its assurance activities ensures that at least one guarantor loan is included in its selected sample for testing.

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 434 breaches of Part 8 of the Code for Period 2. In the previous reporting period, banks reported 447 breaches of Part 8 of the Code.

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

Code Chapter	Number of breaches Period 1 Jun–Dec 19	Number of breaches Period 2 Jan–Jun 20	Number of breaches 12 months
30 Keeping your accounts safe and secure	10	1	11
31 Statements we will send you	16	15	31
32 Cost of transaction service fees	18	29	37
33 Managing a credit card	62	13	75
34 Direct debits and recurring payments	147	240	387
35 Joint Accounts	32	51	83
36 Closing any of your banking services	114	36	150
37 Your right to copies of certain documents	13	9	22
38 When we change our arrangements with you	35	40	75
Total	**447**	**434**	**871**

Banks reported a wide range of incidents as breaches under Part 8. 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. Some customers were referred to the merchant to cancel a direct debit instead of the bank actioning their request. The BCCC is conducting further monitoring activities into this issue. Other examples of breaches included banks not following processes correctly such as closing customers' accounts without a reasonable notice or not following the correct transaction dispute process.

Banks reported that most of the incidents (68%) were the result of human error. Banks identified Part 8 incidents following complaints from the customer in 39% of cases, followed by self-identified or self-reported by a staff member (23%).

Over 250,000 customers were impacted by the incidents reported under Part 8 of the Code, with a financial impact of over $500,000. The main corrective action taken by banks was staff training, coaching and feedback. Banks primarily remediated customers by way of refund or reimbursement (for 38% of incidents).

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.

Requests for financial difficulty assistance

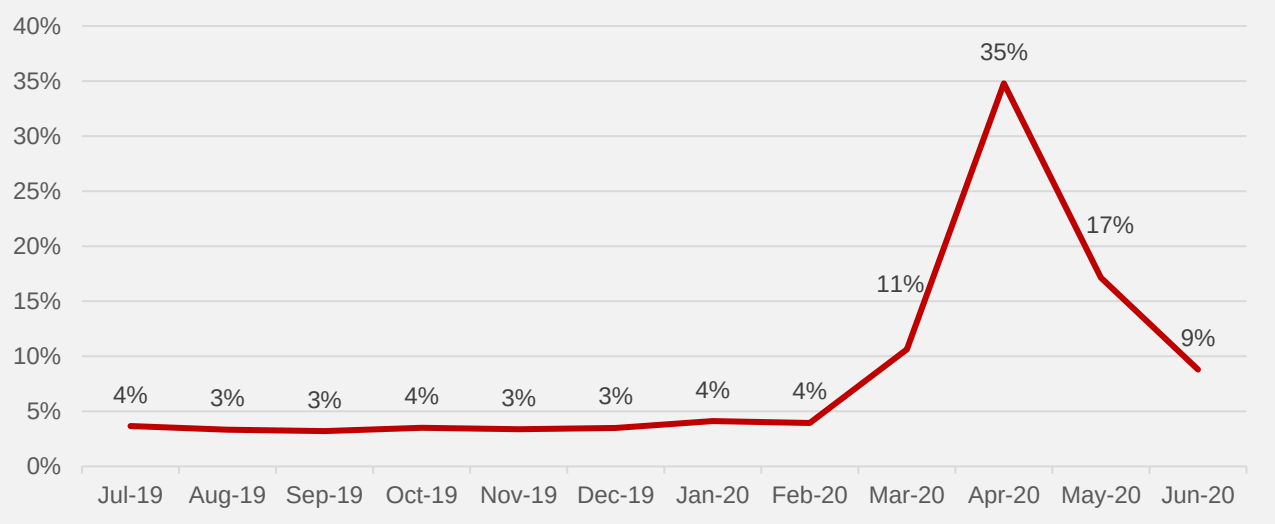
Banks' compliance with their financial difficulty obligations should be understood in the context of the number of requests for financial difficulty assistance that banks receive and grant.

Banks received 351,245 requests for financial difficulty assistance in 2018–19. This increased to 894,112 in 2019–20. While this is unsurprising in light of the impact of COVID-19 on individual and small business customers, the BCCC considers the actual figure is much higher. Several banks excluded the COVID-19 payment deferral packages provided to customers from the financial difficulty data they reported.

This has led to data integrity and consistency issues which impact the BCCC's ability to provide a detailed breakdown of the data.

Nevertheless, as indicated in **Chart 2**, customers' requests for assistance began to increase considerably in March 2020 and peaking in April 2020.

Chart 2: Percentage of total requests for financial difficulty assistance in 2019–20, By Month



The most common forms of financial difficulty assistance provided by banks in 2019–20 were, as one might expect, payment deferrals, followed by repayment arrangements and loan restructuring.

The most common reasons provided for why financial difficulty assistance was not provided to a customer are because a customer did not supply supporting information, the request was withdrawn, or the bank was unable to contact the customer.

Breach data

Banks reported 3,662 breaches overall of Part 9 of the Code for January to June 2020 (Period 2).

Table 8: Breakdown of Part 9 Code breaches, By Chapter

Code Chapter	Number of breaches Period 1 Jun–Dec 19	Number of breaches Period 2 Jan–Jun 20	Number of breaches 12 months
39 Contact us if you are experiencing financial difficulty	1,567	1,004	2,571
40 We may contact you if you are experiencing financial difficulty	123	14	137
41 We will try to help you if you are experiencing financial difficulty	327	392	719
42 When you are in default	6	112	118
43 When we are recovering a debt	1,703	1,886	3,589
44 Combining your accounts	4	13	17
45 Helping with deceased estates	219	241	460
Total	**3,949**	**3,662**	**7,611**

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
  - Record keeping deficiencies
  - Collections activity during an AFCA complaint or where a hardship arrangement was in place
- Deceased Estate delays and errors

Reported breaches of Chapter 45 (Deceased Estates) account for only about 1% of the total number of breaches reported. However, their impact upon customers is high due to the emotion and stress involved.

Examples of breaches include the following:

- For account closures less than $15k as part of deceased estates, these had been closed in branches without a refund or fee reversal being performed. This breach affected 1,186 customers.
- A branch did not act on letters received from a Solicitor in an appropriate manner which resulted in a 2-month delay.

- A bank did not have a process in place that allows it to remove a deceased customer's name from any of the bank's products.
- In one case, a Deceased Estate account was charged fees for more than five years after the bank was notified of the death of the account holder.
- One bank reported a breach whereby a deceased person's guarantee was not revealed to the estate when it tried to sell the deceased person's property. This led to a delay in the settlement of the property.

These breach reports and the BCCC's own observations of overall compliance with Chapter 45 indicate to us that further work needs to be done by banks to meet their Code obligations and the BCCC will likely examine banks' compliance with deceased estates provisions in the near future.

Banks reported that most of the incidents under Part 9 (72%) were the result of human error, 11% were the result of a system failure or issue and while business disruption due to COVID-19 was listed as the cause of less than 4% of incidents, this accounted for 30% of the breaches where further information was provided.

Banks identified Part 9 incidents following complaints from the customer in 18% of cases – the majority were identified by Line 1 monitoring (43%).

Banks' approach to compliance monitoring of financial difficulty and debt collection obligations

Insight into banks' monitoring activities with respect to the debt recovery and financial difficulty obligations contained within Part 9 of the Code indicates that almost all banks undertake monitoring of these key obligations as a combined function with the debt collections resources and framework extending to financial difficulty requirements as well. Nevertheless, banks have provided separate data around monitoring of their financial difficulty obligations.

Bank data indicates that 40% of all Part 9 incidents (including incidents recorded under Deceased estates clauses) were reported through line 1 monitoring. This is in line with the responses provided by the banks on their approach to monitoring debt recovery and financial difficulty requirements. Call monitoring and quality assurance reviews were the most common methods of monitoring employed by the industry, followed by system controls and targeted reviews. Some banks took a multilayered approach by conducting call monitoring within operational teams as well as through their quality assurance teams and as part of end to end file reviews. The monitoring generally was based on random sampling of accounts, but in some cases, banks conducted criteria-based sampling, for example delinquency rate/stage of account or staff performance metrics.

According to the data available the bank recording the highest number of incidents for Part 9 identified 83% of the incidents through its line 1 monitoring function.

However, five banks either did not conduct any call monitoring or did not provide any information about this as part of their response, with one bank's response indicating that no ongoing monitoring of any type was conducted in the period under review. This is of concern to BCCC and individual feedback will be provided.

In addition, there appears to be a considerable reliance by the banks, irrespective of their size, on automated systems in relation to customer interaction, arrears and aging of accounts reporting, correspondence, response timeframes oversight and general reporting. However, in line with the general industry theme, banks have not provided any details on testing conducted on the functionality or performance of the systems that enable this activity. While email or correspondence monitoring is reported as being undertaken by most banks, some banks appear to either have minimal or no oversight of customer correspondence, with emails or letters either system-generated or outsourced to external providers.

Smaller banks tend to centralise the hardship approval process with senior management or credit risk committees with no independent monitoring or oversight reported.

Only two of the banks provided information on monitoring of debt collection or third-party agents. Chapter 43 of the Code requires any external parties engaged by the bank to comply with the relevant guidelines and the BCCC strongly encourages banks to maintain ongoing oversight of the external parties accordingly.

Banks generally apply a relationship management approach to business customers experiencing financial difficulty with targeted reviews also being undertaken.

Examples of good practice initiatives:

- One of the major banks undertook a mystery shopping exercise across its branch and call centre staff to monitor staff understanding of their need to identify and offer assistance to customers who maybe experiencing financial difficulty and vulnerability related to specific clauses of the Code.
- Monitoring of enforcement process: While recognising customers may experience additional difficulty and vulnerability during this stage of the recovery process, the bank ensures that the recovery process is compassionate, and considers whether the proposed enforcement action is fair, reasonable and ethical through the use of an 'ethical checklist' that considers alternate options, adherence to laws and Code provisions and any special circumstances not previously known before going through a sign-off process with senior executives.
- Another bank follows a similar process whereby a specialist team is engaged to conduct a fairness review independently prior to any mortgage enforcement.
- To ensure consistency in approach and outcomes on the subjects of vulnerability and financial assistance a monthly call calibration session is held with the appropriate leaders/staff members where a sample of relevant calls is reviewed. This also serves as an awareness and learning session.
- Another bank undertakes reviews at least once every month on aged delinquent accounts to ensure 'unlikely to pay' indicators are reviewed and appropriate action is taken. 'Unlikely to pay' refers to a situation in which it is unlikely that the customer will pay their obligations in full due to the financial difficulty the customer may currently be having or is likely to have in the immediate future. The review also highlights delays with regard to the management of these cases which are as a result of knowledge gaps or performance.

Impact of COVID-19 on monitoring activities

While acknowledging the unexpected challenges resulting from the pandemic and the rapid adjustments made by the banks, the BCCC is encouraged to observe that 11 out of the 19 banks undertook some form of COVID-19 impact themed review that directly related to the debt collection and financial difficulty obligations. Examples are targeted reviews of impacted loans to identify any additional support required by customers, analysis of debt collections/financial difficulty complaints, home loan deferral audits and COVID-19 process controls testing.

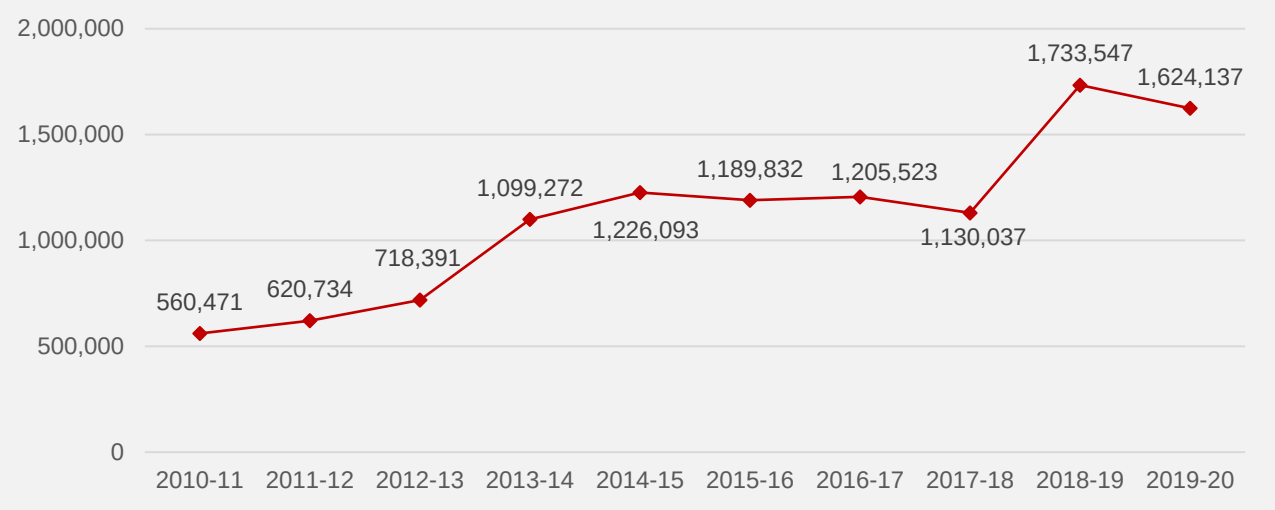
Also, one of the banks reported increasing its monitoring capacity significantly in response to the increase in financial difficulty requests and collections activity as a result of COVID-19. While the banks had to reallocate resources to adjust to the challenges, only four of the banks reported any reduction or cessation of their overall compliance monitoring activities.

Part 10 – Resolving your complaint

Customer complaints

Banks resolved 1,624,137 complaints in 2019–20, a 7% decrease from the 1,733,547 complaints resolved in 2018–19. In line with the previous seven years of reporting to the Committee, one major bank accounts for the majority of complaints – 70% of the total in 2019–20. Chart 3 provides the total number of complaints reported by banks since 2010–11.

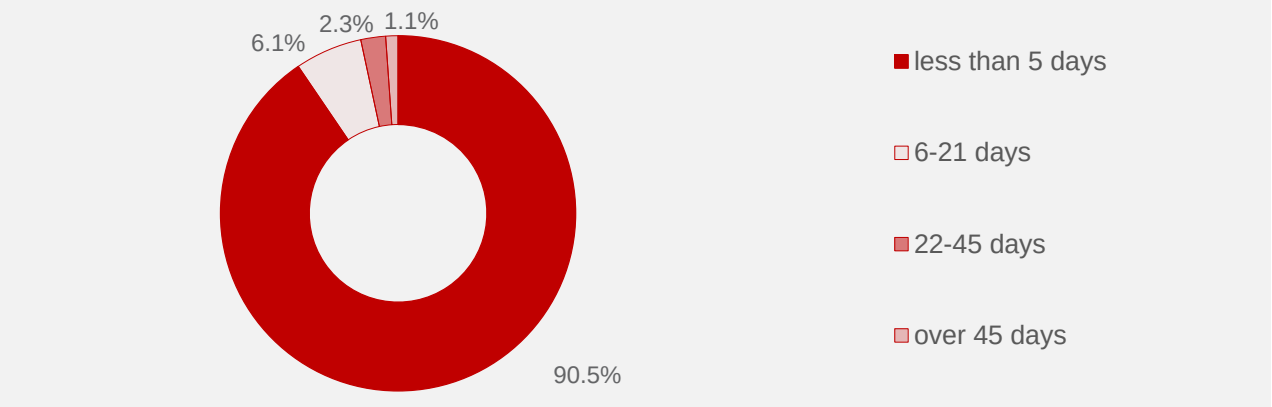
Chart 3. Complaints resolved, 2010–11 to 2019–20[7]



ASIC's current Regulatory Guide (RG165) permits banks to not record complaints that are resolved to the customer's complete satisfaction within five business days. As the BCCC has previously reported, some banks capture and report all expressions of dissatisfaction received, while others do not.

Banks resolved 90% of all complaints within five working days (**Chart 4**), consistent with 2018–19.

Chart 4. Complaint resolution timeframes, 2019–20

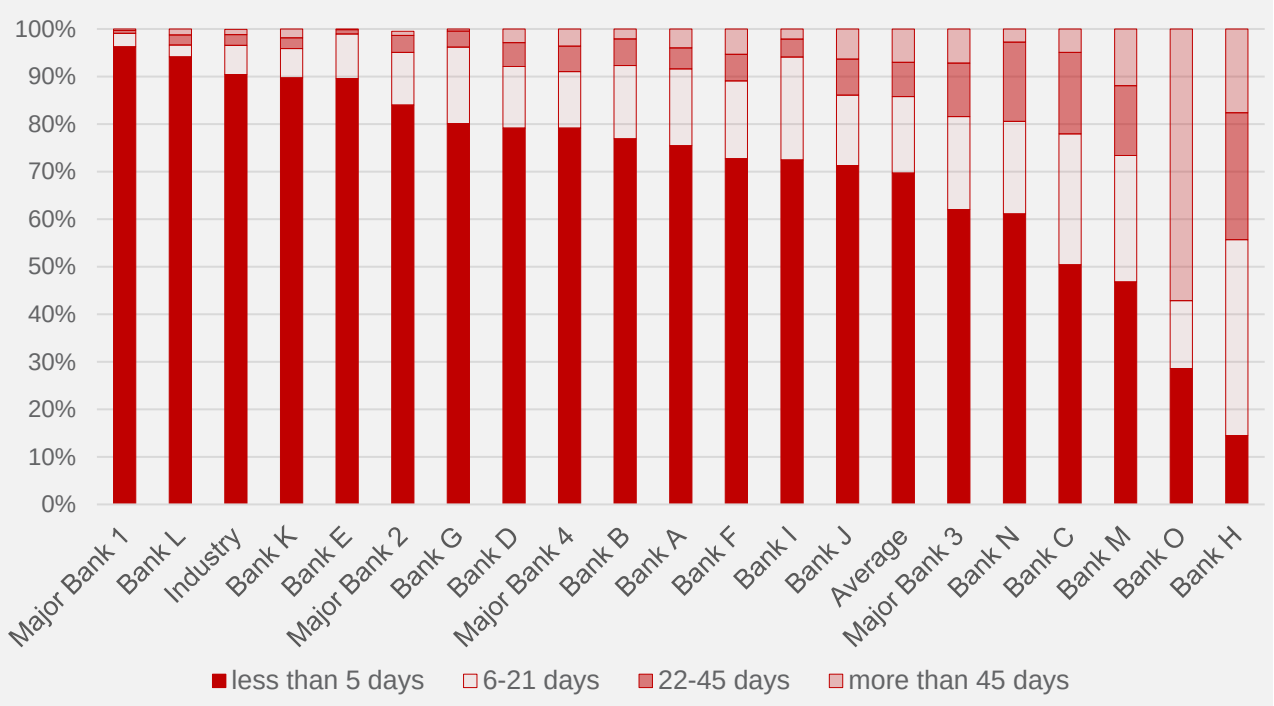


[7] Data for 2011–11 to 2018–19 includes the 13 subscribers to the 2013 Code. 2019–20 data covers the 19 subscribers to the current Banking Code. The six new subscribers account for 1% of the total number of complaints for 2019–20.

In October 2021, ASIC's new Regulatory Guide (RG 271 - *Internal dispute resolution)* will come into effect and ASIC is working with the industry to establish a standardised data regime for customer complaints which will likely lead to more consistent data being provided to the BCCC.

As indicated in **Chart 5** below, there are marked differences in complaint resolution timeframes between banks. Chart 5 also shows 'Industry' and 'Average' figures. The 'Industry' figure is calculated using the total number of complaints reported by all 19 banks. The 'Average' figure is the mean average of each individual bank's percentage for each resolution time period.

Chart 5. Complaint resolution timeframes, by bank, 2019–20



Transaction accounts and payments were the most complained about product (19% of complaints) in 2019–20, followed by credit cards (18%) and home loans (16%). 22% of complaints did not relate to a specific product.

Complaints were most commonly about customer service or bank staff (34%), and rates, fees, charges or pricing (21%), consistent with previous years.

Breach data

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 1,206 breaches overall of Part 10 of the Code for the period July to December 2020 (Period 2), in comparison to 1,248 breaches for the previous period (Period 1).

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. Other breaches occurred where a bank did not provide contact details for AFCA within complaint correspondence.

Banks reported that the vast majority of the incidents (90%) were the result, at least in part, of human error. Consequently, banks reported that they corrected breaches predominantly through staff training, coaching or feedback (85%).

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

Banks identified Part 10 incidents following line 1 monitoring activities 51% of the time. Staff self-reported the incidents in 28% of cases.

Banks' approach to compliance monitoring of complaints handling obligations

Similar to Part 9, banks primarily conduct monitoring over adherence to the internal dispute resolution (IDR) obligations through quality assurance and call monitoring reviews with some dependency on automated or system generated reporting to monitor response timeframes.

Banks apply varied approaches in the application of these methods as part of their frameworks, with some undertaking end to end reviews of closed complaints, while some apply a combination of file and call reviews concurrently, monitoring across a centralised QA team in addition to monitoring by frontline teams with others only independently reviewing escalated complaints via their Customer Advocate functions.

One bank reported reviewing high risk complaints plus a random sample of all other complaints as part of their monitoring while another smaller bank project manages all complaints through to resolution.

Incident identification for complaints handling was found to be largely through proactive methods with 38% of incidents being detected through line 1 monitoring across the 12-month period, followed closely by 37% through self-identification, indicating a high level of awareness of complaints handling obligations among staff. The percentage of incidents identified through the self-identification channel was the highest of the five obligations under review for their monitoring approaches.

While all banks reported conducting some form of monitoring, four of the banks did not provide any details or conduct any specific complaints related call monitoring activity during the period under review. The BCCC will raise this as part of the individual feedback communicated to these banks.

Bank responses indicate extensive use of automated systems to facilitate the IDR process such as case management tools, system exception reporting (for example, aging of complaints) and correspondence generation. However, only one bank reported undertaking any monitoring or testing of its automated systems in use.

While all banks undertook monitoring on resolved complaints, only three banks reported conducting ongoing reviews of active or live complaints.

A significant number of banks completed or planned to undertake enhancements to their overall complaints handling capabilities and processes with the largest four banks in the

process of implementing the actions identified through ASIC's Close and Continuous Monitoring IDR Review.

In relation to reporting of IDR monitoring outcomes, all banks were found to be undertaking regular reporting of assurance activities and emerging issues to senior management through appropriate forums, which in most cases also served as escalation points.

Examples of good practice initiatives:

- Thematic hindsight reviews conducted on closed complaints by one of the banks focuses on the IDR approach employed to identify opportunities to improve processes and capabilities that support fair outcomes. These reviews target products, issues or customer demographics (for example, older or remote customers) that may carry a higher risk of inconsistent or unfair outcomes or where a complaint could have a material customer impact.
- Another bank holds a monthly 'Scams Governance Forum' led by the fraud team with key stakeholders of the bank including compliance and product to discuss scam related complaints. This forum decides on remedial action to improve future outcomes and develop initiatives to reduce customer liability and subsequently scam related complaints.
- Three banks reported undertaking a 100% peer to peer check of all IDR correspondence prior to sending out the final response to customers as a means of obtaining assurance on the accuracy of content, adherence to timeliness and overall compliance with the related obligations.

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