BCCC
Banking Code
Compliance Committee

BCCC Report

Compliance with the Code of Banking Practice 2018–19

Banks' Annual Compliance Statement results

November 2019

Table of Contents

Message from the Independent Chair

As the Independent Chair of the Banking Code Compliance Committee (BCCC), it is my pleasure to present this report on Code subscribing banks' (banks) compliance with the 2013 Code of Banking Practice (the 2013 Code) in 2018–19.

This report sets out the findings from our analysis of banks' responses to the final Annual Compliance Statement (ACS) under the 2013 Code. The report is an opportunity for the BCCC to both report on industry's ability to comply with and report on the 2013 Code, and to use these results to assess future challenges as banks transition to the 2019 Banking Code of Practice (the 2019 Code).

While there are indications that reporting has improved since 2017–18, questions remain about banks' ability to identify, record and report breaches of the Code. A considerable amount of work will need to be done if banks are going to meet the BCCC's expectations for the new reporting standards of the 2019 Code.

What are banks self-reporting?

The 15,597 Code breaches that banks reported in 2018–19 affected at least 9 million customers and had a financial impact of more than $90 million. Banks reported breaches of 33 different provisions of the 2013 Code ranging from provision of credit (4,066 breaches) to family law proceedings (4 breaches). The total number of breaches is a 54% increase from the previous reporting period, with the number of impacted customers rising by 167%.

Banks also updated the BCCC on breaches that remained under investigation in 2017–18, providing details of both an additional 300,000 affected customers and an extra financial impact of over $110 million.

Banks continue to report the highest number of breaches in privacy and confidentiality and provision of credit. Both obligations saw increases in reported breach numbers since 2017–18.

Two areas that also saw significant increases in breach numbers were internal dispute resolution and financial difficulty. These two areas are now among the top five breach categories. The BCCC has long had concerns about bank compliance in these areas and, considering the significant changes taking place in the regulatory landscape for these provisions, will continue to monitor closely.

In last year's report, the BCCC challenged banks to take a more proactive approach to remediating breaches, and to place affected customers at the centre of these efforts. Banks appear to have improved in this area, providing details of customer remediation for 76% of breaches, up from 39% in 2017–18. While some banks appear to have gone the extra mile to remediate customers, it is apparent that banks still remediate customers far less often than addressing their own process issues. The BCCC considers that there is more work to be done in this area.

Does this accurately reflect banks' conduct?

The 2017–18 report raised concerns about banks not sufficiently reporting breaches. In 2018–19, banks reported more breaches and those breaches include a wider range of 2013 Code obligations. It remains unclear whether the rise in breaches reflects increased non-compliance with the Code, or simply better identification and reporting of breaches.

The BCCC considers there is some evidence however of better identification of breaches by banks. This is reflected in certain provisions, such as internal dispute resolution and financial difficulties.

Despite this, the BCCC remains concerned about the quality of some banks' compliance frameworks and their ability to identify, record and report Code breaches.

Breach numbers for certain provisions remain low and vary significantly from bank to bank. For some provisions, it is unlikely that the low number of breaches reflects industry conduct. Certain banks for instance did not report any direct debit breaches, despite the BCCC's own independent monitoring indicating that it was highly likely that these banks will have breached the Code at some point in the last 12 months.

The trend of reporting breaches of Code provisions that mirror legislative obligations continued. Examples include the high number of reported breaches of the privacy and confidentiality, provision of credit and debt collection obligations. Few banks report on breaches of the Code's more nuanced, unique requirements - despite the thousands of customer interactions covered every day by the 2013 Code.

Even for breaches that were reported, the consistency of reported data remains an ongoing area of concern. The BCCC found consistency issues with the recording of complaints, and the number of requests for financial difficulty assistance received and approved. The BCCC will continue to engage with industry and provide further guidance to enhance the level of consistency in all areas of reporting.

The BCCC is also aware that, in some instances where banks have improved breach identification and reporting, this is likely due to banks committing resources to this area for transition to the new Code, or because of inquiries made by the BCCC – not because of ongoing robust risk and compliance frameworks. Inquiries made by the BCCC throughout 2018-19 have led to hundreds of extra beaches being reported in this year's ACS. The BCCC is concerned that banks would not have identified these issues if not specifically required to do so.

In the Financial Services Royal Commission final report, Commissioner Hayne outlined that the purpose of industry codes was to 'set standards on how to comply with, and exceed, various aspects of the law'. To ensure that industry codes work effectively, the Commissioner noted that there must be 'adequate means to identify, correct and prevent systemic failures in applying the code.'[1]

Banks are required to report on every single identified breach of the Code. While this in some ways is an ambitious goal, it is a goal that banks should strive to achieve. The BCCC believes they are falling short.

What does this mean as we transition to the 2019 Banking Code?

This ACS confirms the BCCC's belief that banks need to make significant improvements to ensure they comply with the 2019 Code, and to accurately report when they fall short of meeting its obligations.

The 2019 Code contains several new provisions not covered in the 2013 Code, and banks have demonstrated here that certain reported practices would continue to be a breach of several new provisions. The BCCC has found this in several of the case studies highlighted in this Report.

[1] Commonwealth, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, *Final Report* (2019) vol 1, 107.

The new Code also has more stringent reporting requirements. Banks are required to report information to the BCCC every six months. At this stage, the Committee is concerned about banks' ability to report timely, accurate data within these timeframes.

The BCCC challenges banks to act quickly to ensure they comply with the new Code, and to record and report in a timely and appropriate manner when they do not.

The BCCC will keep banks focused on breach identification and reporting to ensure they meet the commitments they have made to their customers.

Prof. Christopher Doogan AM FIML FAICD
Independent Chairperson
Banking Code Compliance Committee

Introduction

This report summarises banks' compliance with the 2013 Code in 2018–19. It is based on results from the ACS, the primary compliance monitoring activity for the 2013 Code. The ACS enables the BCCC to benchmark banks' compliance with the 2013 Code, report on current and emerging compliance issues and identify priority areas for future monitoring.

On 1 July 2019, the 2013 Code was replaced by the 2019 Code. This report focuses on the 2013 Code whereas future breach data from compliance statements will relate to the 2019 Code.

The Code Compliance Monitoring Committee (CCMC), the body that monitored compliance with the 2013 Code, was also replaced by a new body, the Banking Code Compliance Committee (BCCC).

The BCCC

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

To do this, the BCCC will:

- examine banks' practices
- identify current and emerging industry wide problems
- recommend improvements to bank practices
- consult with and keep stakeholders and the public informed.

The BCCC carries out any work previously initiated by the CCMC.

Monitoring banks' compliance with the Code

A key part of the BCCC's role is to monitor banks' compliance with the Banking Code. Our comprehensive monitoring program incorporates regular self-reporting by banks, major and targeted inquiries, and investigation of potential breaches of the Code. The BCCC monitors compliance with the 2013 Code and 2019 Code, as well the previous 2004 Code of Banking Practice (where appropriate).

The BCCC encourages banks to have a positive culture of self-reporting. This includes taking responsibility for identifying and reporting breaches and making practice improvements to prevent future breaches. We publish the results of this data and use it to identify problems and advise banks on where they can improve.

To make the best use of our resources, we focus our monitoring on the most important issues – particularly ones that are industry wide, serious or systemic.

Summary of approach

The ACS was the major data collection activity for the 2013 Code. The ACS program was conducted in accordance with clauses 5.1(e) and 5.2 of the previous CCMC Mandate. The 2018–19 ACS enables the BCCC to:

- benchmark banks' compliance with the 2013 Code
- report on current and emerging issues in Code compliance to the industry and wider community, and
- establish the areas of highest priority for its future monitoring work.

The 2018–19 ACS built on the improved collection methods of the previous year's ACS. The 2017–18 ACS saw major improvements that substantially increased the detail of the breach data collected. This resulted in receiving more appropriate and detailed data from the ACS and the 2018–19 ACS continued this method of collection.

The 2018–19 ACS required each Code-subscribing bank to report the total number of Code breaches it identified during the reporting period. Banks were then asked to provide further detail about breaches meeting 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 $1000 on a customer
- the nature, cause and outcome of more than one breach is the same.

In addition, the ACS asked banks to report details for a random sample of 5% of the remaining breaches of each Code clause.

While the collection method of this year's ACS was similar to previous years, there were some minor adjustments. Principally, banks were required to provide details separately for the remediation steps they took:

- for affected customers, and
- to prevent recurrence.

In previous years, the CCMC observed that when correcting a breach, banks tended to focus on preventing recurrence, rather than addressing the breach's impact on a customer. By requesting a

separate response for each issue, this year's ACS sought to obtain greater clarity on how and when banks remediate breaches of the Code.

For the 2019 Code, the ACS will be replaced by a new data collection activity, the Banking Code Compliance Statement (BCCS). This will be collected biannually in accordance with clause 4.2 of the BCCC Charter.

Analysis and discussion

After analysing the ACS data, the BCCC provided each bank with a copy of this report, benchmarking it against the industry. The BCCC will also meet with each bank to discuss this report and the outcomes of the 2018–19 ACS.

The Report

Like the 2017–18 ACS, the data in this report has been de-identified. All bank names are replaced by placeholders, such as Bank A, except for the largest four banks which are referred to as "Big 4" or "Major bank". Banks are not labelled consistently throughout, for example Bank A in one section will not be labelled Bank A in another section.

As noted above, banks provide the overall number of breaches, and then provide further details for a significant sample of these. As a result, the total figures for the breaches in which details have been provided is lower than the total number of breaches reported. Further details can be found in each chapter below.

Insights from our priority areas

The BCCC has outlined three key priority areas for 2019–20. These are:

- customers experiencing vulnerability
- small business and agribusiness, and
- transition to the new Code.

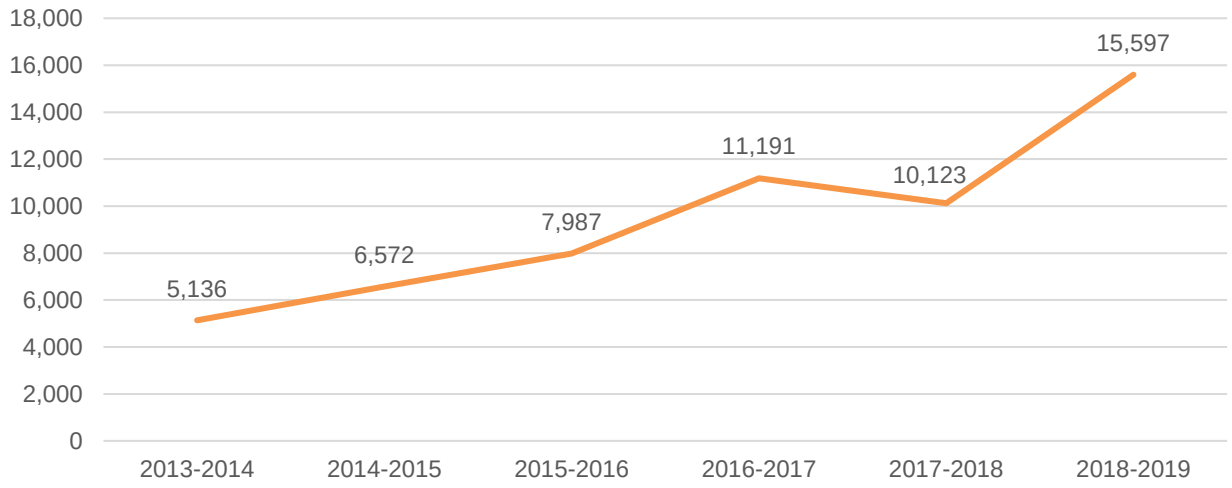
The BCCC is not convinced that these issues are reported adequately by banks, and this has contributed to them being BCCC priorities for the coming year. The BCCC has identified examples of breaches of these priorities in 2018–19, which we have provided as case studies. These serve to demonstrate the importance of the priorities.

Breaches overall

Breach trends

Banks reported 15,597 breaches in 2018–19, a 54% increase from 10,123 breaches in 2017–18. This figure is 39% higher than the most breaches ever previously reported in an ACS, which was 11,191 in 2016–17.

Chart 1. Code Breaches, 2013–14 to 2018–19



While the main Code clauses that are most commonly breached have been constant, there has been a significant rise in breaches of clause 37 – Internal Dispute Resolution. For the first time, breaches concerning financial difficulties is also one of the top five breach categories of the Code.

Figure 1. Top five Code breach categories, 2014–15 to 2018–19

2014–15	2015–16	2016–17	2017–18	2018–19
Privacy and confidentiality (1,795)	Provision of credit (2,328)	Provision of credit (4,178)	Privacy and confidentiality (4,464)	Privacy and confidentiality (4,821)
Provision of credit (1,318)	Privacy and confidentiality (2,108)	Privacy and confidentiality (2,743)	Provision of credit (2,489)	Provision of credit (4,066)
Compliance with Laws (1,126)	Compliance with Laws (1,114)	Debt collection (2,061)	Debt collection (725)	Internal Dispute Resolution (2,432)
Debt collection (589)	Debt collection (796)	Compliance with Laws (632)	Compliance with Laws (594)	Debt collection (1,289)
Internal Dispute Resolution (538)	Key Commitments (555)	Key Commitments (472)	Internal Dispute Resolution (419)	Financial Difficulties (714)

This year saw significant increases in Code breaches by nearly all banks. Several banks reported over double the number of breaches previously provided.

For the first time, the four largest reporters of breaches are the Code's largest four banks.

Table 1. Code breaches, by bank, 2014–15 to 2018–19

Bank	2014–15	2015–16	2016–17	2017–18	2018–19	Change 2018–19
Big 4	3,592	4,832	8,064	5,848	8,539	46.02%
Big 4	365	912	800	718	2,331	224.65%
Big 4	309	210	320	1,060	1,212	14.34%
Big 4	390	450	420	455	1,108	143.52%
Bank A	1,095	975	649	875	867	-0.91%
Bank B	21	152	168	447	639	42.95%
Bank C	31	82	240	283	377	33.22%
Bank D	131	177	258	145	134	-7.59%
Bank E	465	100	146	151	127	-15.89%
Bank F	17	24	31	44	89	102.27%
Bank G	9	31	30	39	80	105.13%
Bank H	147	41	62	58	79	36.21%
Bank I		1	3		15	
Total	**6,572**	**7,987**	**11,191**	**10,123**	**15,597**	**54%**

Following the ACS' reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 13,081 breaches – 84% of the total reported. The rest of this chapter refers only to this subset of breaches.

What caused the breaches

Banks reported that the clear majority of breaches (93%) had a single cause, with 6% of breaches having multiple causes. In addition, no cause was reported for the remaining breaches.
Where a single cause or multiple causes were reported:

- 91% involved human error
- 8% involved a system error
- 4% involved a control, training or resourcing failure, including process deficiencies

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 responsible for addressing compliance risk. While the model is applied in different ways by banks, generally it features the:

- first line, comprising business management responsible for day-to-day risk management, decision-making involving risk identification, assessment, mitigation, monitoring and management
- second line, comprising the specialist risk management function that is independent of the first line and develop risk management policies, systems and processes among other tasks, and
- third line, consisting of independent assurance providers such as internal audit.[2]

Occasionally, banks have stated that the issues were identified through review, but not provided indication of which line identified the issue. In these instances, the BCCC has stated that the issues were identified by 'internal review'.

A significant majority of breaches were identified by Line 1 quality assurance activities including call monitoring (74%). This is an increase from 2017–18, where 65% of breaches were identified in this way. The other main methods of breach identification were:

- complaint or customer query (9%)
- review by the second line of defence (6%)
- self-identified or reported by a staff member (4%)
- internal review (3%).

The impact of the breaches

Banks reported that 13,081 breaches in 2018–19 impacted more than nine million customers, with a total financial impact of around $90 million. The number of customers impacted has increased by approximately 167% since those first reported in the 2017–18 report, while the financial impact has decreased by 5%.

As banks have not finished investigating all breaches, the actual impact will be greater. This was demonstrated last year, when further investigation of breaches still under investigation in 2017–18 found considerably greater impact. More details can be found in the final chapter of this report, *Updates to breach details since 2017–18*.

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

Table 2. Impact of Code breaches, by bank, 2018–19

Bank	Total Breaches	Customers Impacted	Financial Impact
Big 4	8,434	1,345,119	$18,956,996.00
Big 4	2,278	3,811,014	$37,735,182.59
Big 4	701	1,531,869	$26,483,098.82
Bank A	401	977,566	$4,616,783.00
Big 4	386	142,887	$1,272,019.24
Bank B	328	22,768	$964,146.00
Bank C	236	314,580	$220,185.00
Bank D	134	3,583	$223,085.84
Bank E	79	594,688	$8,082.00
Bank F	60	459,733	$56,411.00
Bank G	17	19,804	$2,500.00
Bank H	15	10,113	$18,470.00
Bank I	12	14	$32,000.00
Total	**13,081**	**9,233,738**	**$90,588,959.49**

Table 3. Impact of Code breaches, by Code obligation, 2018–19

Code Obligation	Breaches	Customers Impacted	Financial Impact
27 Provision of credit	3,811	116,901	$11,715,066.49
24 Privacy and confidentiality	3,538	1,612,601	$828,491.21
37 Internal dispute resolution	2,399	4,667	$4,580.00
32 Debt collection	1,220	86,883	$219,418.09
28 Financial difficulties	670	2,525	$228,095.60
3 Key commitments	412	1,093,599	$27,348,297.07
12 Terms and conditions	221	867,891	$1,553,682.39
4 Compliance with laws	183	3,645,274	$35,974,291.22
39 Availability of information about dispute resolution processes	149	149	$0.00
31 Guarantees	95	5,996	$9,655,637.92
9 Staff training and competency	84	2,843	$2,422,270.00
21 Direct debits	74	69	$48,926.00
26 Statements of account	37	157,826	$165,329.14
35 Electronic communications	30	199,013	$0.00
14 Cost of credit	26	783	$270,105.81

Code Obligation	Breaches	Customers Impacted	Financial Impact
33 Closure of accounts in credit	24	67	$38,975.80
22 Chargebacks	22	1,370,775	$18,063.00
11 Availability of copies of the Code	17	0	$0.00
13 Copies of documents	8	7	$550.00
20 Changes to terms and conditions	8	5,552	$14,520.00
7 Customers with special needs	7	5	$1,000.00
16 Account suitability	7	7	$15,113.00
19 Account combination	7	58,982	$2,506.83
23 Information relating to foreign exchange services	6	79	$877.00
30 Joint accounts and subsidiary cards	6	6	$31,510.00
18 Pre-contractual and new account information	4	1,003	$12,990.00
29 Joint debtors	4	5	$11,560.00
25 Payment instruments	3	3	$3,275.07
40 Family law proceedings	3	0	$0.00
8 Customers in remote Indigenous communities	2	219	$2,512.85
15 Operation of accounts	2	7	$1,315.00
34 Branch closure protocol	1	0	$0.00
38 External dispute resolution	1	1	$0.00
Total	**13,081**	**9,233,738**	**$90,588,959.49**

How the breaches were corrected

This year, the most common way breaches were corrected was by seeking to prevent their recurrence. In 98% of breaches, the banks took steps to prevent recurrence. Banks addressed the impact of a breach on a customer for 76% of breaches.

While banks continue to remediate the customer's impact of a breach significantly less frequently than taking steps to prevent recurrence, both are significant improvements from 2017–18. In 2017–18, banks reported that they had taken preventive action for 76% of breaches but had addressed the individual customer impact for only 39% of breaches.

To prevent breaches from recurring, banks had:

- provided staff training, coaching or feedback (9,800 breaches)
- enhanced monitoring or controls (2,685)
- reviewed or improved processes (2,072)
- reviewed staff performance or taken disciplinary action (2,027), and
- implemented a system fix (252).

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

- communicated or corresponded with the customer (4,228)
- corrected the individual issue, including updating details (2,974)
- apologised to the customer (1,094)
- logged, managed or resolved a complaint (1,092)
- refunded or remediated a customer (1,004)
- requested that information be destroyed, deleted or returned (431)

Provision of Credit

Clause 27 of the 2013 Code required banks to exercise the care and skill of a diligent and prudent banker when forming an opinion on a customer's ability to repay a credit facility.

Each bank has its own internal policy and procedure which it considers meets the requirements to act as a diligent and prudent banker. Most of the breaches detailed in this section involve a bank identifying that it has failed to act in line with these internal standards, and reporting this as a breach of the Code.

The BCCC notes however that there is considerable debate on what constitutes diligent and prudent lending. As a result, while a bank may consider that its internal policy and procedure is compliant, it still could be in breach of its Code obligations.

Breach trends

Banks reported 4,066 Provision of Credit breaches in 2018–19. This is a significant 63% increase from 2017–18, where banks reported 2,489 breaches. This figure is more aligned to that reported in 2016–17, where banks reported 4,178 breaches.

Ten banks reported breaches of clause 27 in 2018–19, an increase from the nine that did so in 2017–18. Eight banks saw an increase in provision of credit breaches, while two reported a decrease.

Consistent with previous years, one outlier bank reported most of these breaches (2,612, 64%), although the proportion of the overall breaches provided by the outlier bank has been decreasing (from 80% in 2017–18 and 93% in 2016–17).

The significant increase in breaches can be attributed partially to the outlier bank, which saw its breaches increase in 2018–19. The bank stated that the increase was primarily due to changes in its file review team process. These changes, initiated to improve accuracy and consistency, identified a significant increase in provision of credit breaches.

The increase can also be attributed to another Big 4 bank, which saw its breaches increase to 996 in 2018–19, from a mere 58 in the previous year. The bank's low number of reported breaches in 2017–18 was the subject of an inquiry by the CCMC in 2019. Because of this investigation, the bank found that it was not fully utilising all possible avenues of inquiry to identify provision of credit breaches, such as hindsight, quality control and mortgage file compliance reviews. Fully utilising such avenues saw a significant increase in identified breaches. The bank also said that the rise was partially due to increased quality assurance reviews in its contact centre.

Table 4. Provision of Credit breaches, by bank, 2017–18 to 2018–19

Bank	2017–18	2018–19	Change 2018–19
Big 4	1,981	2,612	32%
Big 4	58	996	1,617%
Big 4	175	171	-2%
Bank A	56	125	123%
Big 4	29	67	131%
Bank B	185	51	-72%
Bank C	1	25	2,400%
Bank D	-	7	-
Bank E	-	7	-
Bank F	2	5	150%
Bank G	2	-	-
Total	**2,489**	**4,066**	**63%**

Following the ACS' reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 3,811 breaches – 94% of the total reported. The rest of this chapter refers only to this subset of breaches.

The nature of the breaches

Provision of credit breaches were primarily the result of two main factors.

Processing or system error

2,298 breaches (60%) were primarily the result of a processing or system error. This includes:

- 1,646 breaches were the result of one bank identifying that the documents it had filed in its systems did not support elements of lending decisions.
- 524 breaches were due to a bank becoming aware that telephone credit application processes were not followed correctly, and
- 83 breaches were due to banks becoming aware that debt consolidation discussions had not been conducted correctly.

Not responsible or incorrect lending decision

1,417 breaches (37%) were due to irresponsible or incorrect lending decisions. Where further detail could be ascertained, 304 breaches were due to a customer's financial situation being incorrectly calculated or recorded. 251 breaches related to instances where employees had not followed bank policy.

What caused the breaches

Banks overwhelmingly considered provision of credit breaches to be the result of human error. 3,686 breaches (97%) were considered at least partially to be the result of human error. In comparison, a mere 84 breaches were attributed to a control, training or resourcing error.

How the breaches were identified

A majority of Provision of Credit breaches were identified through line 1 monitoring or quality assurance (2,903 breaches, 76%). Breaches were also identified by one or more of the following:

- Line 2 monitoring (742)
- Complaint or customer query (73)
- Internal review process (45)
- Australian Financial Complaints Authority (AFCA) / Financial Ombudsmen Service (FOS) (40)
- Self-identified or reported by a staff member (32)

The impact of the breaches

Breaches of the Provision of Credit clause of the 2013 Code had a significant impact. Over 110,000 customers were impacted, with a financial impact of nearly $12 million. Both figures are a significant increase from 2017–18, where approximately 12,000 customers were impacted with a financial impact of $8.4 million.

Table 5. Impact of Provision of Credit Breaches, 2018–19

Bank	Breaches	Customers Impacted	Financial Impact
Big 4	2,567	4,410	$242,000.00
Big 4	995	1,632	$4,283,503.00
Bank A	61	124	$6,946.00
Bank B	51	69	$2,070,118.00
Big 4	45	49,109	$4,517,107.28
Big 4	43	54,389	$324,478.82
Bank C	25	6,068	$157,764.00
Bank D	14	8	$113,149.39
Bank E	7	52	$0.00
Bank F	3	1,040	$0.00
Total	**3,811**	**116,901**	**$11,715,066.49**

One big 4 bank impacted nearly 53,000 customers with a systemic breach. In this example, the bank identified that for certain credit limit increases it was using out of date processes, principally automated behavioural scoring, and therefore did not:

- make inquiries about the customer's current and actual financial situation,
- verify the customer's income, or
- make inquiries or use the customer's credit bureau credit file.

The bank states the remediation for customers for this matter is still ongoing. To address the immediate issue and prevent recurrence, the bank initiated a system fix.

Another Big 4 bank impacted nearly 12,000 customers when a system error caused errors in certain applications for a credit card or personal loan. These errors resulted in problems with the serviceability assessment that led to income being incorrectly calculated. The bank states it had contacted affected customers and is improving its procedures to prevent recurrence.

The biggest financial impact was of $1,000,000, a breach that also impacted up to 10,000 customers. In this instance, certain home loan amalgamations were being processed without a serviceability assessment being carried out. The bank has stated it is improving its processes to address this issue.

How the breaches were corrected

Banks reported a range of measures to correct Provision of Credit breaches, but as identified in previous years, banks tended to place heavier emphasis on preventing recurrence than on remediating affected customers. For 3,741 breaches (98%), banks corrected the breach at least in part by seeking to prevent recurrence. This is opposed to 3,371 breaches (88%) where at least in part the breach resulted in remediation for the customer. Both are equal or above the average for remediation of breaches more widely in 2018-19.

When banks sought to remediate the customer, banks generally either communicated with the customer (2,265 breaches) or corrected the individual issues or details (967). Significantly less frequently, banks refunded or reimbursed a customer (103).

When banks sought to prevent recurrence, they prioritized three main solutions. Most commonly, they enhanced monitoring or controls (2,294). Second most common was the introduction of a staff performance management program (1,660), although this is potentially artificially high as one set of 1,646 breaches from one Big 4 bank was all partially remediated in this way. Third most common was staff training, coaching or feedback (1,295).

Guarantees

The guarantee provisions under clause 31 contained some of the 2013 Code's most prescriptive and unique requirements. These included detailed provisions on the information a bank should provide to a potential guarantor, such as notices (for example, that the guarantor should seek independent legal and financial advice), and supporting information (for example, copies of credit contracts, credit reports and statements of accounts). It also outlined that banks should allow a potential guarantor until the next day to consider the information provided. The Code set out obligations relating to how the guarantee is signed and how guarantors can withdraw from a guarantee.

In the last year, the BCCC has received notification of potentially systemic breaches of the guarantee provisions of the 2013 Code. Based on this understanding of guarantee practice, the BCCC is concerned that breaches of the Code may be significantly more than those reported by banks in the ACS.

To address this, the BCCC is currently conducting an extensive inquiry into guarantees, seeking to understand how banks employ guarantees for the credit they offer and their processes for ensuring compliance with the guarantee provisions.

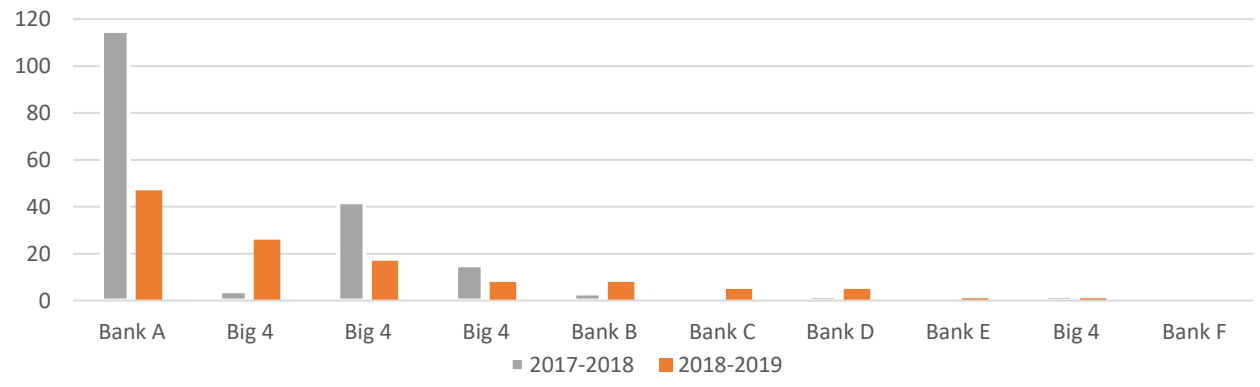
Breach trends

Banks reported 118 guarantees provisions breaches, a 35% decrease from 184 breaches reported in 2017–18. However, this is still a notable increase from the 36 breaches reported in 2016–17.

The decrease from 2017–18 can be attributed largely to one bank. Bank A, while still reporting the highest number of guarantees provisions breaches, saw their number of breaches decline by 68. This is a 60% decrease from 2017–18.

One Big 4 bank saw a 550% increase in breaches from 4 to 26. This bank did not provide a reason for the increase. This was an exception to the remaining Big 4 banks, which between them saw an average decrease of 48% in guarantees breaches. Four banks did not report any breaches of the guarantees provisions.

Chart 2. Guarantees provisions breaches, by bank, 2018–19



Following the ACS reporting instructions, banks provided further information about the nature, cause, impact and correction of 95 guarantees breaches – 80% of the total guarantees breaches reported. The rest of this report chapter refers only to this subset of 95 breaches.

The nature of the breaches

A significant majority of guarantees breaches (85%) detailed a failure to provide the required disclosures or prominent notices to a potential guarantor. This is a slight increase from 2017–18, which saw 77% of breaches occur due to similar reasons. This result continues to demonstrate the issues faced by banks in ensuring prospective guarantees receive the required disclosures and notices.

Banks reported that in 15 cases (16%), they did not properly assess the suitability of a guarantor. Additionally, 11 breaches (12%) related to the execution of the guarantee itself, including guarantors not being provided with adequate time (at least the next day) to consider the guarantee documents. These breaches also included providing the guarantee documents to the borrower to arrange signing, rather than directly to the guarantor.

Transition to the New Code – Case Study

Clause 31 – Guarantees

Through the transition to the new 2019 Code, a bank discovered it had not been complying with parts of Clause 31.4 relating to guarantees in the 2013 Code. The bank was not providing potential guarantors with a copy of any related credit report of the debtor as required under this clause.

The bank has investigated the credit contracts where this Code sub-clause was not complied with and has confirmed that none of these loans are with the collections team or in financial hardship. The bank will continue to undertake further monitoring of these contracts.

The bank has updated its guarantor process so that it is compliant with the 2019 Code.

What caused the breaches

Process issues, including issues with controls, training or resourcing, accounted for 56 (59%) of the guarantees breaches. This is above the trend for ACS breaches, suggesting these processes are a key risk area for compliance with the Guarantee provisions. A quarter of the breaches identified were due to human error.

How the breaches were identified

More than half of the guarantees breaches were identified through Line 1 monitoring activities.

Table 6. Identification of guarantees breaches, 2018–19

Breach identification method	Breaches	Percentage of Breaches
Line 1 Monitoring / System monitoring / quality assurance	54	57%
Complaint/customer query	18	19%
AFCA / FOS	9	9%
Self-identified or reported by staff member	8	8%
Internal Review	5	5%
External party	1	1%
Total	**95**	**100%**

The impact of the breaches

The 95 breaches relating to guarantees impacted at least 5,996 customers. Most of this figure was due to one Big 4 bank detailing 3,099 affected customers from eight breaches. The total financial impact was just over $9.5 million, a considerable increase from the $819,331 financial impact recorded in the 2017–18 financial year. This is caused by a financial impact of $9,561,251 provided by one Big 4 bank for its 26 breaches.

In the 2017–18 ACS, the CCMC raised its concerns about how the impact of guarantees breaches was being reported. That year, only one bank reported any financial impact at all in relation to its guarantee breaches.

While more banks are reporting the financial impact of guarantees breaches, the BCCC has continued concerns over this data and considers banks have likely understated the customer and financial impact of guarantees breaches. For example, a Big 4 bank considers only three customers were financially impacted, despite breaching the guarantee provisions 17 times. Likewise, Bank A breached the guarantee provisions 47 times, impacting 172 customers, but did not report any financial impact.

The BCCC maintains its belief that in cases where a guarantee is not enforced, banks are not reporting financial impact data, on the basis that it is the bank rather than the customer that bears this impact. In addition, banks had previously informed the CCMC that when assessing financial impact, they have not considered any additional fees or costs associated with entering a defective guarantee.

Table 7. Impact of guarantees breaches, 2018–19

Bank	Breaches	Customers Impacted	Financial Impact
Bank A	45	172	$0.00
Big 4	26	924	$9,561,251.00
Big 4	8	3,099	$0.00
Bank B	5	5	$0.00
Bank C	3	5	$62,538.00
Big 4	3	3	$31,848.92
Bank D	2	7	$0.00
Big 4	2	1	$0.00
Bank E	1	1,780	$0.00
Total	**95**	**5,996**	**$9,655,637.92**

How the breaches were corrected

Banks' steps to address guarantees breaches emphasised preventing recurrence. There were 73 (77%) breaches where the bank sought to prevent recurrence, with 42 (44%) relating to addressing an individual customers impact. This is a significant increase from the mere seven breaches in 2017–18 that addressed the customer's impact.

The main actions taken to prevent recurrence were implementing one or more of the following corrective actions:

- process improvements, review or enhanced controls (54 breaches)
- staff training, coaching or feedback (15)
- implementing a 'consequence', disciplinary action or performance management for the staff member involved (5).

These are a significant change from 2017–18. Last year, 86% of breaches were addressed with staff training, coaching or feedback whereas only 4% of the breaches were addressed through process improvements, review or enhanced controls.

Banks appear to be addressing the root cause process or control issues leading to breaches. Six of the nine banks who reported guarantees breaches addressed at least one breach in this way. The BCCC considers this an important step in addressing guarantees issues that are a result of process or control failure.

The main actions to remediate customers were implementing one or more of the following actions:

- customer refund or reimbursement (20 breaches)

- customer apology or communication (15)
- the individual issue was corrected (9)
- releasing the guarantor from the guarantee or deeming it unenforceable (8).

More banks appear to be addressing customer impact. The BCCC and its predecessor, the CCMC, have argued that banks should reflect on the standing of a guarantee when correcting and reporting on a breach.

The BCCC notes, however, that many breaches still did not address the status of the guarantee itself, and that banks released the guarantor from the guarantee, or deemed it unenforceable, in only a handful of cases. The BCCC considers that more work needs to be done in this area.

Debt Collection

The 2013 Code's debt collection obligations were set out in clause 32 and stated:

- banks will comply with the ACCC and ASIC Debt Collection Guideline: for Collectors and Creditors and will take all reasonable steps to ensure that bank representatives also comply
- if a bank sells a debt to a third party, it will choose a third party that agrees to comply with the guideline
- a bank will not assign a customer's debt, except as part of a funding arrangement such as securitisation or the issue of covered bonds, while:
  - it is actively considering the customer's financial situation where the customer is in financial difficulty
  - a customer is complying with an agreed financial difficulty repayment arrangement.

Breach trends

Banks reported 1,289 debt collection breaches in 2018–19. This is a 78% increase from 2017–18, where banks reported 725 breaches. This figure is closer, though still significantly less, than that reported by banks in 2016–17, where banks reported 2,061 breaches.

Consistent with previous years, one outlier bank reported most of these breaches (687, 53%). While its absolute number of breaches increased in 2018–19, from 476 to 687, the proportion of the overall breaches provided by the outlier bank has been dropping in recent years (from 65% in 2017–18 and 96% in 2016–17).

The outlier bank stated the absolute rise was due to continued focus on this obligation through call monitoring, which has identified high volumes of these incidents. The bank stated that it has continued to develop its call monitoring process and the understanding of this obligation through collaboration between its quality assurance and compliance teams.

Also, one Big 4 bank saw a significant rise from 3 to 206 breaches. The banks low number of reported breaches in 2017–18 was the subject of an inquiry by the CCMC in 2019. As a result, the bank conducted further analysis and ascertained it had not fully reviewed its complaints data and quality monitoring mechanism in relation to breaches of this clause, and as a result it had been underreporting. This enhanced focus led to the bank identifying significantly more breaches in 2018–19.

Table 8. Debt Collection breaches, by bank, 2017–18 to 2018–19

Bank	2017–18	2018–19	Change 2018–19
Big 4	476	687	44%
Big 4	206	280	36%
Big 4	3	206	6,767%
Bank A	16	43	169%
Big 4	17	34	100%
Bank B	-	21	-
Bank C	6	14	133%
Bank D	-	2	-
Bank E	-	1	-
Bank F	1	1	0%
Total	**725**	**1,289**	**78%**

Following the ACS' reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 1,220 breaches – 95% of the total reported. The rest of this chapter refers only to this subset of breaches.

The nature of the breaches

As was the case in 2017–18, inaccurate or incomplete file notes was the main breach type, accounting for 54% of debt collection breaches. The provision of incorrect information, including the misrepresentation of consequences, accounted for 17% of debt collection breaches.

Table 9. Debt Collection Breaches by type, 2018–19

Type of incident	Breaches	% of breaches
Incomplete or inaccurate file notes	661	54%
Incorrect information provided in arrangement negotiations or misrepresentation of consequences	212	17%
Unnecessary contact with customer	125	10%
Collection activity on accounts where it was inappropriate (for example payment arrangement, bankruptcy, deceased and settlements)	112	9%
Failure to comply with debt collection guidelines	40	3%
Other	70	6%
Total	**1,220**	**100%**

What caused the breaches

As has been the case in previous years, an overwhelming majority of breaches were caused, at least in part, by human error (1,158 breaches). This year has seen a significant number of breaches although also attributable in part to a system failure or error (583). A control, training or resourcing error was also a minor cause cited (61).

The impact of the breaches

Debt Collection breaches impacted over 86,000 people, with a financial impact of approximately $220,000.

Table 10. Impact of Debt Collection breaches, 2018–19

Bank	Breaches	Customers Impacted	Financial Impact
Big 4	687	46,672	$0.00
Big 4	264	3,581	$13,530.56
Big 4	204	526	$40,305.81
Big 4	27	35,280	$160,324.72
Bank A	18	134	$0.00
Bank B	14	679	$5,257.00
Bank C	3	7	$0.00
Bank D	2	2	$0.00
Bank E	1	2	$0.00
Total	**1,220**	**86,883**	**$219,418.09**

One Big 4 bank accounted for the largest customer impact of 46,672. Despite this, the same bank claimed that there was no financial impact for these affected customers.

34,970 customers were affected by one large breach by a Big 4 bank. In this instance, a review of the credit card collection strategy identified that some customers were receiving SMS messages more regularly than the contact guideline. The bank chose not to remediate customers but implemented a system fix. The cause of the incident remains subject of investigation.

How the breaches were corrected

When banks breached the debt collection provisions, they overwhelmingly focused on remediation by preventing recurrence (1,185 breaches, 97%). They often did so exclusively, with remediation for the customer significantly less common (350 breaches, 29%). This low level of customer remediation is significantly below that of the average of Code breaches in 2018–19.

When banks sought to prevent recurrence, they focused heavily on one primary form of correction: staff training, coaching or feedback (1,118 breaches). While significantly less common, banks also occasionally would correct through one or more of a system fix (38) or process review or improvements (25).

Where banks remediated the customer, they implemented a greater range of remediation options, primarily one or more of the following:

- individual issue corrected (247 breaches)
- customer apology (80)
- communication with customer (17), and
- customer refund or reimbursement (15).

Financial Difficulty

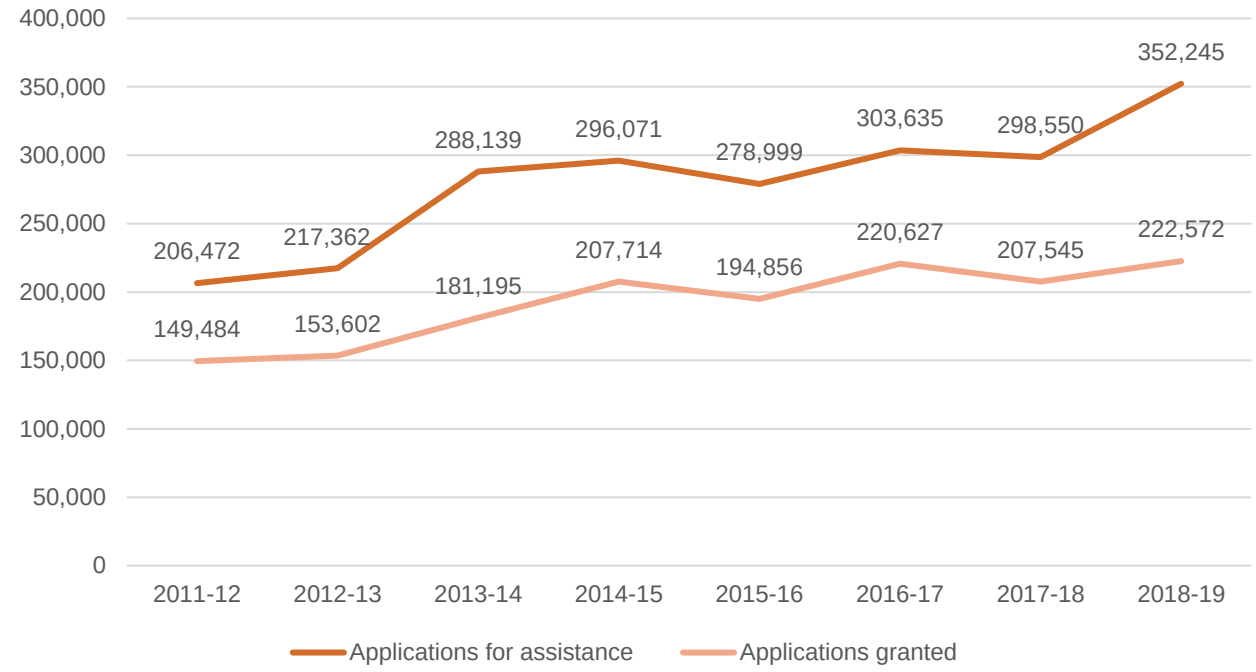
Banks' financial difficulty obligations were set out in clause 28 of the 2013 Code. The Code states that banks must try to help customers overcome their financial difficulties with any credit facility they have with their bank.

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.

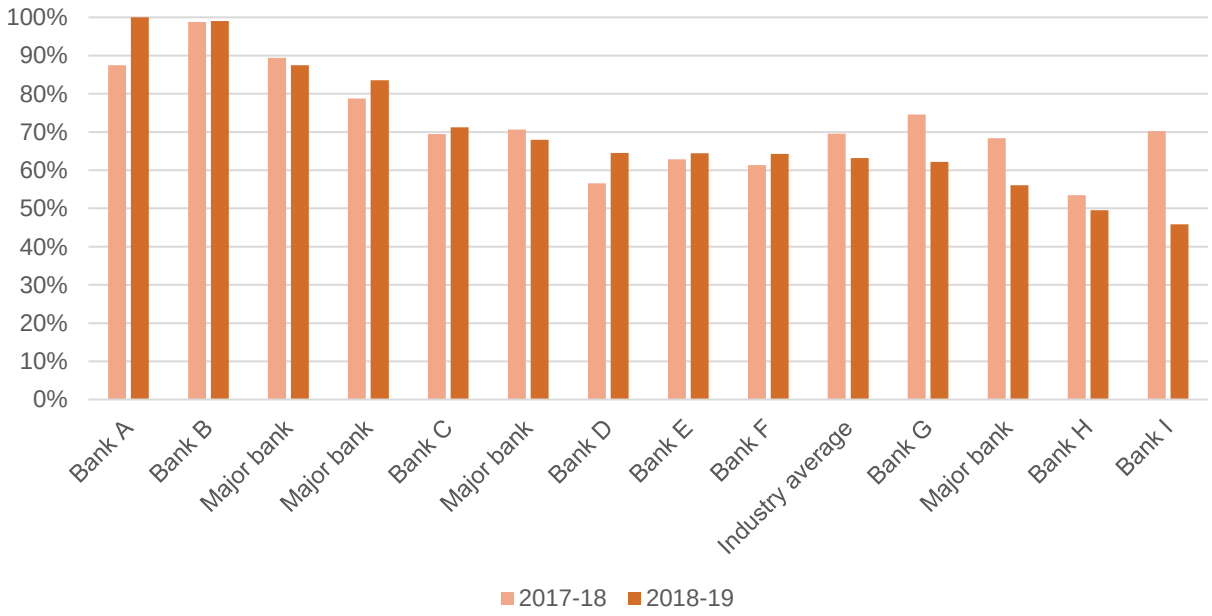
Banks received 351,245 requests for financial difficulty assistance in 2018–19, a 18% increase from 298,550 requests in 2017–18 (Chart 3). Ten banks reported increases – ranging from 4% to 82% – while three banks saw the number of requests for assistance decrease.

Chart 3. Requests for financial difficulty assistance received and granted, 2011–12 to 2018–19



There is a substantial variation between banks in terms of the rate of assistance granted. The rate of assistance at one big 4 has decreased significantly in the last 12 months.

Chart 4. Percentage of requests for financial difficulty assistance granted, by banks, 2017–18 and 2018–19*



* Banks A and B receive the lowest number of requests for assistance (both fewer than 250 requests).

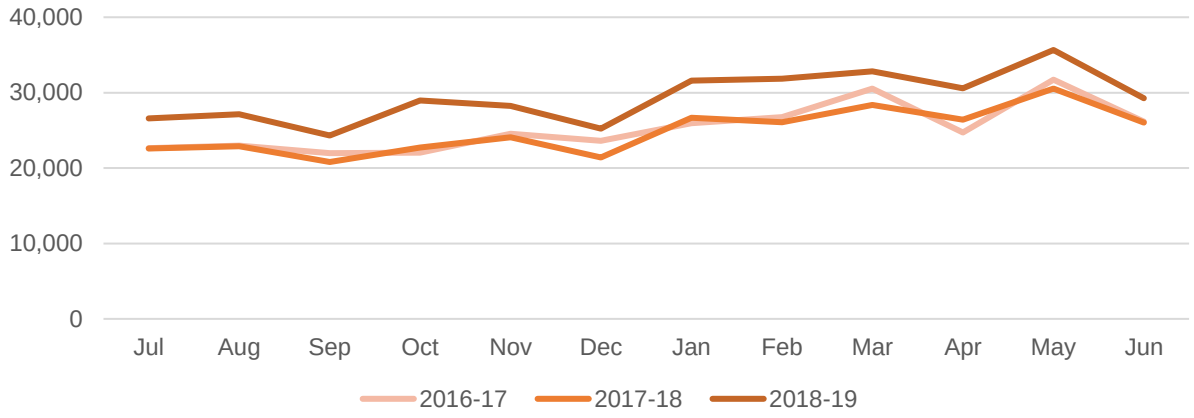
Banks granted assistance on 222,572 occasions – an overall assistance rate of 63% (Table 11). This is a 6.3% decrease from 69.5% in 2017–18 and is the second lowest rate of assistance since the CCMC began collecting this data in 2012.

Table 11. Percentage of requests for financial difficulty assistance granted, 2011–12 to 2018–19

2011–12	2012–13	2013–14	2014–15	2015–16	2016–17	2017–18	2018–19
72.4%	70.7%	62.9%	70.2%	69.8%	72.7%	69.5%	63.2%

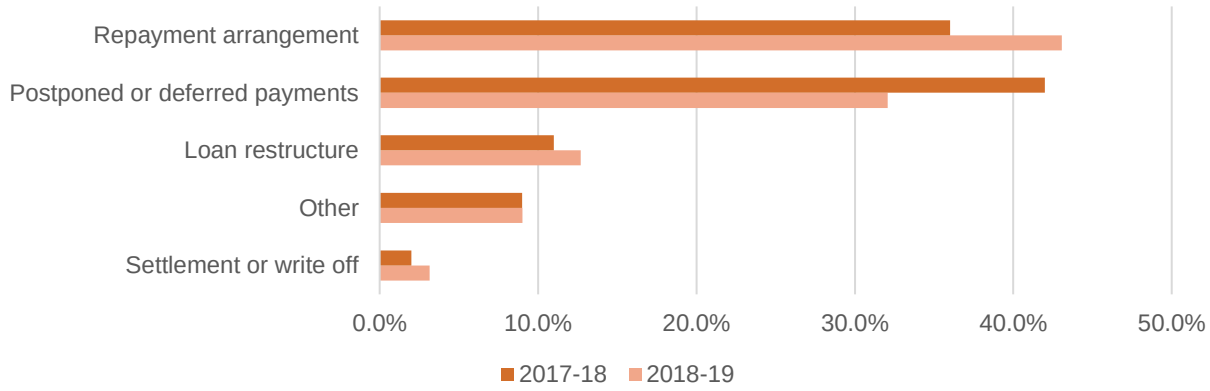
Chart 5 displays the total number of requests for assistance received by month for 2016–17, 2017–18 and 2018–19. The trend is broadly similar for these three reporting periods and indicates that the number of requests received, tends to be higher and fluctuates from month to month towards the end of the financial year.

Chart 5. Requests for financial difficulty assistance received, by month, 2016–17 to 2018–19



The most common forms of financial difficulty assistance granted by banks in 2018–19 were repayment arrangements (43.1%) and postponed or deferred payments (32.1%), a reversal in order from 2017–18 (Chart 6).

Chart 6. Types financial difficulty assistance provided, 2017–18 and 2018–19



When banks did not provide financial difficulty assistance, this was most often because the customer did not supply supporting information (70%), consistent with previous reporting periods. The Committee raised this as a concern in its 2018 Financial Difficulty Inquiry Report and made several recommendations to banks to address this issue. The BCCC will monitor closely whether this remains the leading reason financial difficulty assistance is not provided in 2019–20.

Breach trends

Banks reported 714 financial difficulty breaches in 2018–19, a 335% increase from 164 in 2017–18 (Table 12). This overall increase can largely be attributed to increases reported by eight banks, and two big 4 banks in particular.

The big 4 bank that reported the most financial difficulty breaches attributed the increase to a continued focus on the obligations through call monitoring in direct channels and financial difficulty teams. The bank has continued to improve the call monitoring process and the monitoring team's understanding of the financial difficulty obligations.

The other big 4 bank saw a significant rise from 27 to 285 breaches. *A CCMC investigation into reported breaches in 2017–18 meant that the bank conducted a review and identified it had underreported breaches of clause 28 because of a process error, and because it was not utilising an existing internal report in order to identify breaches.* This enhanced focus led to the bank identifying significantly more breaches in 2018–19.

Table 12. Financial difficulty breaches, 2017–18 to 2018–19

Bank	2017-18	2018-19	Change 2018–19
Big 4	51	289	467%
Big 4	27	285	956%
Big 4	31	46	48%
Bank A	12	30	150%
Bank B	6	17	183%
Bank C	16	16	0%
Bank D	7	13	86%
Big 4	6	11	83%
Bank E	4	5	25%
Bank F	4	2	-50%
Total	164	714	335%

Following the CCMC's reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 670 financial difficulty breaches – 94% of the total financial difficulty breaches reported. The rest of this report chapter refers only to this subset of 670 breaches.

The nature of the breaches

The largest contributor to financial difficulty breaches, accounting for 72% of the total, was the failure to action a request for assistance, or to do this within the required timeframe. These types of breach accounted for 43% in 2017–18. A further 20% of breaches occurred when a bank did not identify or follow up financial difficulty indicators.

Table 13. Types of financial difficulty breach, 2018–19

Issue	Breaches	Percentage of breaches
Financial difficulty assistance requests not actioned or responded to within timeframe	484	72%
Potential financial difficulty triggers not identified and/or followed up	136	20%
Financial difficulty assistance request not processed correctly or genuinely considered	26	4%
Other (including not engaging with customer's authorised representative and debt collection activity taking place while financial difficulty assistance was being considered or an arrangement was in place	24	4%

Customers experiencing vulnerability – Case study

Clause 28 – Financial difficulty

Under the Code, banks have an obligation to assist customers who have a credit facility if they are experiencing financial difficulty. If the banks identify that a customer is experiencing financial difficulty, the bank may contact them to discuss their situation and the options available to them.

A bank reported that its front-line staff were failing to recognise indicators of customers in financial difficulty. During telephone calls with staff, customers would say they needed an overdraft facility so they could purchase food, or they were unable to find work due to illness or injury. Other examples included advising the bank of their concerns about isolation or lack of contact with their family. The bank's staff were not taking appropriate action upon hearing about a customer's situation.

These breaches were considered to be the result of human error and were identified through quality assurance reviews. The bank has undertaken staff training, coaching and feedback to help staff identify and follow up on indicators of financial difficulty.

What caused the breaches

Most financial difficulty breaches (60%) were caused, at least in part, by human error. After this, system error, failure or issue accounted in part for 40% of breaches.

How the breaches were identified

The majority of the financial difficulty breaches (84%) were identified, at least in part, through quality assurance and call monitoring. Bank staff reported a further 10% of breaches. Sources outside the bank also played an important role in the identification of financial difficulty breaches: 6% were identified via customer complaints or queries, FOS/AFCA, or regulators.

The Impact of the breaches

Banks reported that 2,525 customers were impacted by financial difficulty breaches. The financial impact on customers of these industry breaches stands at $228,096.

Table 14. Impact of financial difficulty breaches, 2018–19

Bank	Breaches	Financial Impact	Customers Impacted
Big 4	289	-	1,045
Big 4	282	$69,614	303
Bank A	19	-	19
Bank B	17	-	45
Bank C	16	-	18
Big 4	15	$29,079	921
Bank D	13	-	117
Bank E	12	$36,560	17
Big 4	6	$92,842	39
Bank F	1	-	1
Total	**670**	**$228,096**	**2,525**

How the breaches were corrected

In correcting financial difficulty breaches, banks placed more emphasis on preventing recurrence than addressing the impact on individual customers. For example, one bank reported 107 breaches where potential financial difficulty triggers were not identified or appropriately referred. The bank confirmed that feedback and coaching was provided to a staff member but that there was no customer remediation. In such cases, the bank should ensure (and report to the BCCC) that financial difficulty assistance was eventually discussed with the customer.

Overall, to prevent recurrence, banks most commonly:

- provided staff training, coaching or feedback (for 635 breaches)
- enhanced monitoring and controls (251)
- reviewed or made improvements to processes (34)
- implemented a system fix (2).

To address customer impacts, banks:

- logged and resolved a complaint (251)
- corrected an individual issue (50)
- communicated or corresponded with the customer (42)
- refunded, reimbursed or compensated the customer (22).

There were two breaches subject to ongoing investigation.

Key Commitments

Clause 3 of the 2013 Code required banks to comply with a set of 'Key Commitments'. These were general requirements concerned primarily with how banks would communicate with and inform customers.

Traditionally, the CCMC's compliance monitoring functions and powers only extend to a breach of clause 3 where it is also a breach of another provision of the Code. The CCMC acknowledged that banks may nevertheless wish to record breaches of clause 3 where there is a primary Code breach, without a link to a corresponding breach of other clauses.

The ACS accommodates this approach and consequently some banks (but not all) do report key commitments breaches. A similar approach is taken for breaches of Clause 4 of the 2013 Code – Compliance with laws.

Breach trends

Banks reported 555 Key Commitments breaches in 2018–19, an 84% increase from the 301 breaches in 2017–18, but more closely aligned to the reported number in 2016–17, when 472 breaches were identified.

Table 15. Key Commitment breaches, by bank, 2017–18 to 2018–19

Bank	2016–17	2017–18	2018–19
Big 4	147	61	243
Bank A	2	2	99
Big 4	250	60	66
Bank B	3	53	64
Big 4	23	55	56
Bank C	1	11	16
Big 4	11	-	5
Bank D	3	16	5
Bank E	-	-	1
Bank F	31	27	-
Bank G	-	16	-
Bank H	1	-	-
Total	**472**	**301**	**555**

The overall rise was driven primarily by a significant increase from one big 4 bank who reported 182 breaches more than in 2017–18. This also represented the largest absolute rise overall. However, the bank did not account for the rise.

Bank A reported 99 breaches, after only reporting two in each of the previous years. This bank reported the rise was due to a greater focus on detecting and monitoring breaches of the Code, citing reviews of customers' in-branch and contact centre call experiences. The bank stated that greater focus on call interaction had, in one example, led to an increase in breaches identifying staff providing what is deemed to be financial advice.

Following the ACS reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 412 key commitments breaches – 74% of the total reported. The rest of this report chapter refers only to this subset of 412 breaches.

The nature of the breaches

Key Commitments breaches reflected a wide range of issues such as:

- system or process error (214 breaches)
- failure to act on instructions or account processing issues by staff (147)
- provision of information (24)
- staff misconduct (23)
- CCI sales practices (4).

Small business - Case study

Clause 3 – Key Commitments

A bank reported a breach of clause 3 to the BCCC.

The bank reported that a not-for-profit organisation was not receiving an appropriate account, which has no fees. The bank reported that this indicates that when the customer first joined the bank, inadequate disclosure was made to the customer.

The cause of the breach was unknown, and the breach was identified by staff members of the bank. The bank reported that it remediated the customer by fully refunding all fees and charges. The staff then re-packaged the accounts to the correct setting, so no further fees and charges would be charged.

A sample of Key Commitments breaches from 2018–19

Type of incident	Description of incident	Cause of breach	ID Method	Customer remediation	Actions to prevent recurrence	Customers impacted	Financial impact
System or process error	The bank's approach to charging ongoing fees on bank guarantees in some cases is inconsistent with relevant customer disclosure. Matter reported to ASIC	Design deficiency	Self-identified	Customer remediation is underway with customers to be reimbursed overcharge.	An interim fix is being implemented. The bank is currently developing a systemic fix.	35,000	$8,100,000
System or process error	In some cases, customers whose loans entered and exited a leap year may be charged more interest than implied by their contract.	System error	Internal review	Customer remediation is in progress. The bank’s view is that the financial impact per customer will be small.	In progress	>473,000	Unknown at this stage.
System or process error	Customers are charged an over-drawn fee if they deposit cash into an ATM after 7pm and make a withdrawal before the deposit can be credited to the account.	System error	Customer Complaint	A third party has been engaged to commence customer remediation investigations of impacted customers.	A system fix will be implemented & control review with support by third party.	63,000	$852,000
Human error	External provider emailing non-personal information to external email address.	External provider failure	Self-identified	Not applicable	Provided staff training, coaching or feedback	242,075	0
System or process error	Customers not offered terms and conditions.	System error	Self-identified	Not applicable	Implemented a system fix.	30,027	0

Type of incident	Description of incident	Cause of breach	ID Method	Customer remediation	Actions to prevent recurrence	Customers impacted	Financial impact
System or process error	Failure to manage construction loans remaining on interest only terms.	Deficiency in process & procedure	Self-identified	Customer remediation has not started. The bank will need to identify a target date for commencement of remediation.	A review of the Terms & Conditions to identify if any further changes need to be made to ensure the Terms & Conditions accurately reflect the way the product performs.	12,535	>$1000
System or process error	Closed card details not sent to external card support vendor.	System error	Self-identified	Customer remediation in the form of a refund, compensation or goodwill payment.	Implemented a system fix.	69,279	Unknown at this stage.
Staff misconduct	Staff misappropriation of customer's funds. An investigation found 114 transactions totalling approximately $364,000 across 6 customer accounts to an account used by the staff member. Matter reported to ASIC	Staff misconduct	Customer complaint	Customer remediation, including correcting the issue, apologising to the customers and providing a refund, compensation or goodwill payment	The bank provided staff training, coaching or feedback, reviewed staff performance or took disciplinary action and enhanced monitoring and/or controls	6	$384,000
System or process error	The bank failed to inform customers about the limitations on credit card insurance they had purchased. The policy	Human error	Customer complaint	The charges were refunded.	Not stated	3	$3,882

Type of incident	Description of incident	Cause of breach	ID Method	Customer remediation	Actions to prevent recurrence	Customers impacted	Financial impact
	prevented claims where claimants were on disability pensions or receiving Centrelink support.						
System or process error	Customers were charged a $0.50 fee for certain transactions that apply in relation to certain types of accounts. The fee is not included in terms and conditions.	Human and process error	Self-identified	Customers were remediated.	The product was withdrawn.	2,099	$26,949.25
System or process error	ATM charges to customers not turned off at the same time as the media campaign stating that fees would no longer be charged.	Change management	Not Known	Customer remediation completed.	Implemented system fix to give effect to this fee change campaign.	7,622	$ 14,463

What caused the breaches

Most Key Commitments breaches were caused at least partially by human error (251 breaches or 61%). Banks also cited control, training or resourcing errors for 104 breaches (25%) and system error or issue for 42 breaches (10%).

How the breaches were identified

Banks reported several ways in which the breaches were identified. Customer complaint or query was responsible for the identification of 135 breaches (33%).

Breaches were also identified in one or more of the following ways:

- Line 1 monitoring, system monitoring or quality assurance (82 breaches)
- Self-identified or reported by a staff member (76)
- Line 3 oversight or internal audit (55)
- AFCA / FOS (13).

The importance of the third line in identifying breaches for Key Commitments is high, and breaches identified through this way were considerably higher than the mean across all Code provisions. 13% were identified via the third line, in contrast to less than 2% across the ACS as a whole in 2018–19.

The impact of the breaches

The 413 breaches for which details were provided affected more than one million customers with a financial impact of just over $27 million. One breach accounted for almost half of the customer impact, affecting potentially as many as 473,000 customers. The financial impact was more spread out over several breaches. The largest individual breach with a financial impact was for $8,100,000.

Table 16. Impact of key commitments breaches, by bank, 2018–19

Bank	Breaches	Customers Impacted	Financial Impact
Big 4	201	1,010,659	$14,266,301.41
Bank A	77	395	$1,141,448.00
Bank B	64	80	$9,446.00
Big 4	61	31,387	$1,838,638.66
Big 4	5	51,040	$10,092,463.00
Bank C	4	37	-
Bank D	1	1	-
Total	**413**	**1,093,599**	**$27,348,297.07**

How the breaches were corrected

Banks took steps to address Key Commitments breaches which heavily emphasised on preventing recurrence. They stated that 385 breaches (93%) included a remediation to prevent recurrence, and 306 (74%) involved action to remediate the customer.

Where banks sought to prevent recurrence, they prioritised staff training and feedback for 200 breaches (48%). Process reviews and improvements were also implemented for 69 breaches (16%), and in rare circumstances, staff disciplinary action was taken for 32 breaches (8%).

When banks sought to remediate the customer, banks undertook one or more of the following actions:

- individual issue or details corrected (158 breaches)
- customer refund or reimbursement (115)
- customer apology (61), and
- communication with the customer or correspondence sent (17).

Internal Dispute Resolution

The Internal Dispute Resolution (IDR) obligations under clause 37 of the 2013 Code stipulated that banks must have an internal dispute handling process that is free and accessible, and which meets the standards set out in the Australian Securities and Investments Commission's (ASIC) Regulatory Guide 165 (RG165).

This requirement is replicated in the 2019 Code along with the addition of new obligations including requirements for banks to:

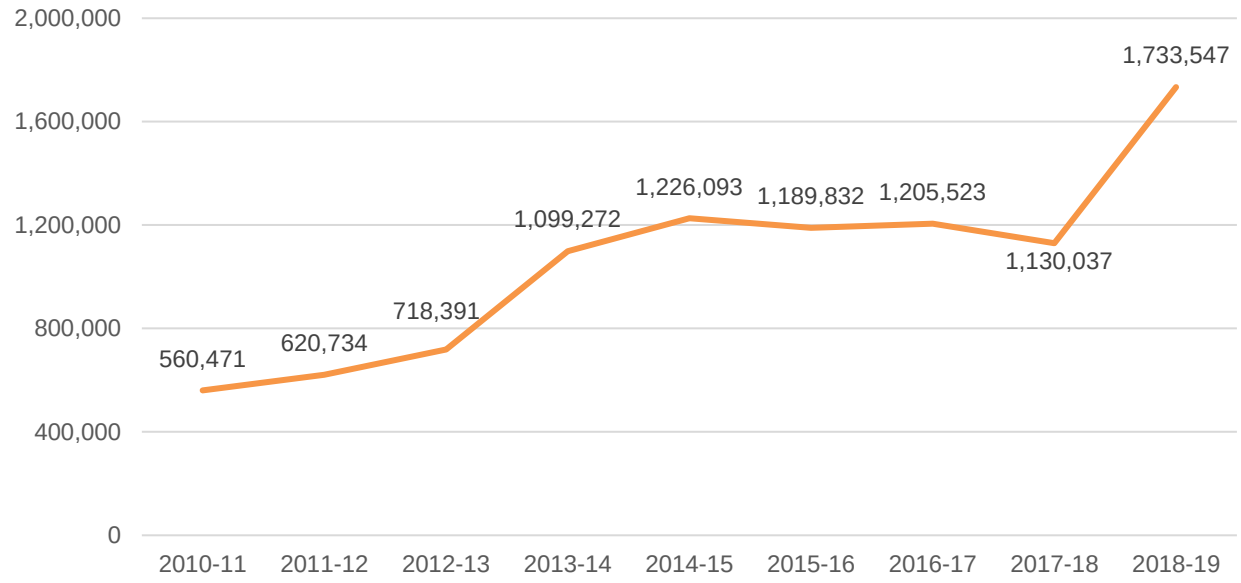
- have a customer advocate
- publish information about its IDR processes
- ensure that the IDR process is fair and reasonable, and
- allow customers to make a complaint to AFCA as an alternative and in addition to farm debt mediation.

Customer complaints

Banks resolved 1,733,547 complaints in 2018–19, a 53% increase from the 1,130,037 complaints resolved in 2017–18. In line with the previous six years of reporting to the CCMC, one big 4 bank makes up most complaints – 58% of the total in 2018–19. This bank's 32% increase in the number of complaints between 2017–18 and 2018–19 largely accounts for the overall increase in complaints over the same period.

Two banks reported significant increases in the number of complaints (1385% and 922% respectively) which also contributed to the overall increase. Eight additional banks reported an increase, while complaints decreased for three banks. One bank's stated belief is that heightened awareness among customers to raise their concerns following the Financial Services Royal Commission may have had an impact on complaint numbers.

Chart 7. Complaints resolved, 2010–11 to 2018–19



ASIC's RG165 permits banks not to record complaints that are resolved to the customer's complete satisfaction within five business days. As the CCMC had previously reported, some banks capture and report all expressions of dissatisfaction received, while others do not. This variation in approach creates inconsistencies in complaint resolution data.

The two banks which reported significant increases in complaints numbers in 2018–19 have changed their approach since last year to now record all expressions of dissatisfaction, including those resolved within five working days.

It is the BCCC's understanding that all banks except for one now record all expressions of dissatisfaction, even if resolved within five days.

The BCCC notes that as of November 2019, ASIC is consulting on proposed changes to complaints handling standards within RG165 and the framework for recording and reporting complaints data to ASIC.

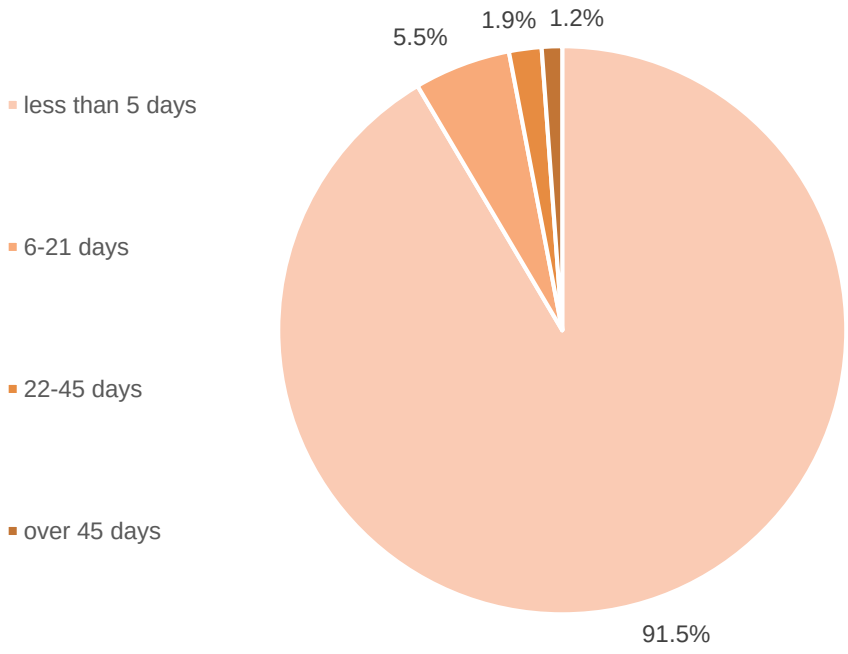
In its submission to the ASIC Consultation Paper 311, the BCCC stated that it supports proposals to impose further requirements on banks regarding complaints data collection for the following reasons:

- Such changes are likely to assist the BCCC achieve its purpose to monitor and drive best practice Code compliance.
- They may lead to the banking industry taking a more consistent approach to complaints handling and the recording of complaints data.
- It would enable the Committee to focus more on the underlying issues of the complaints and work to improve standards of practice and compliance with the Code, rather than focusing on reporting inconsistencies.
- It believes that recording details of all complaints will ensure that banks are able to monitor their compliance with RG165 and consequently the Code's IDR requirements – namely that all complaints have been resolved to a customer's satisfaction.
- It agrees with ASIC's rationale that such data will provide banks with a much deeper source of data to:
  - understand customers' needs and the key drivers of complaints
  - identify emerging issues
  - strengthen data integrity
  - promote greater consistency in data collection practices.

How quickly complaints were resolved

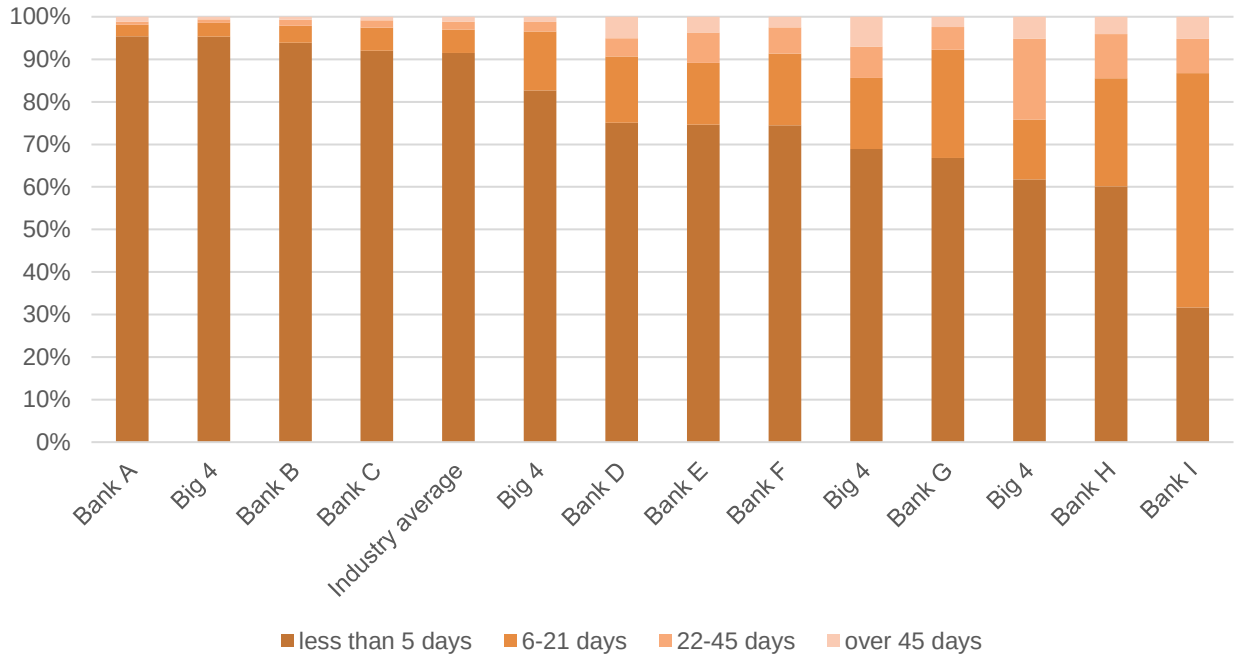
Banks resolved 91% of all complaints within five working days (Chart 8), consistent with 2017–18.

Chart 8. Complaint resolution timeframes, 2018–19



There are marked differences in complaint resolution timeframes between banks. For comparison purposes, Chart 9 also shows an 'industry average' figure, calculated as the mean average of each individual bank's percentage for each resolution time period.

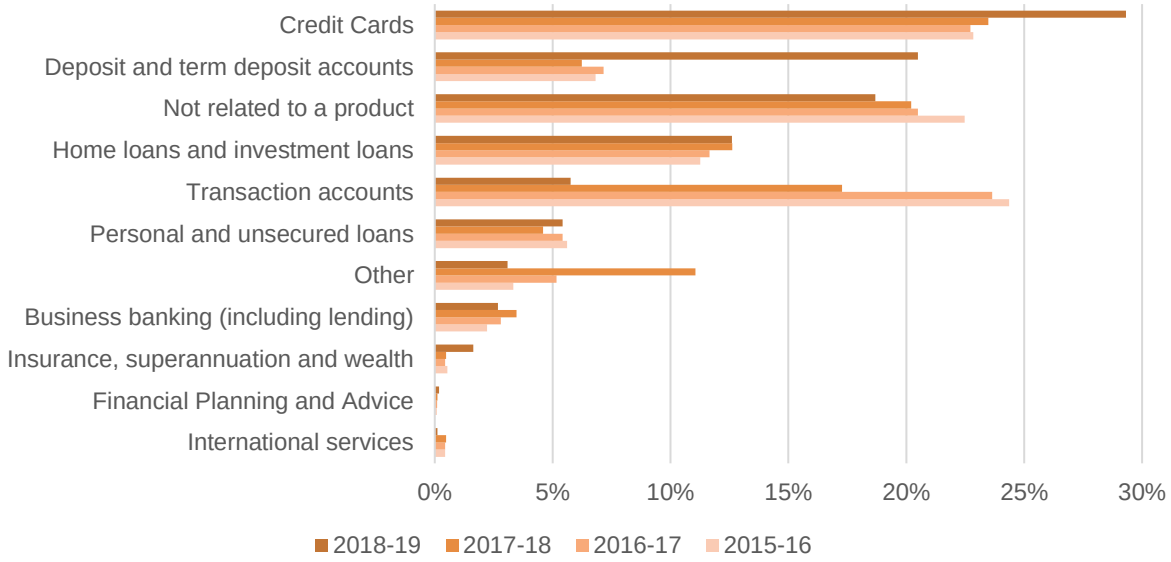
Chart 9. Complaint resolution timeframes, by bank, 2018–19



What customers complain about

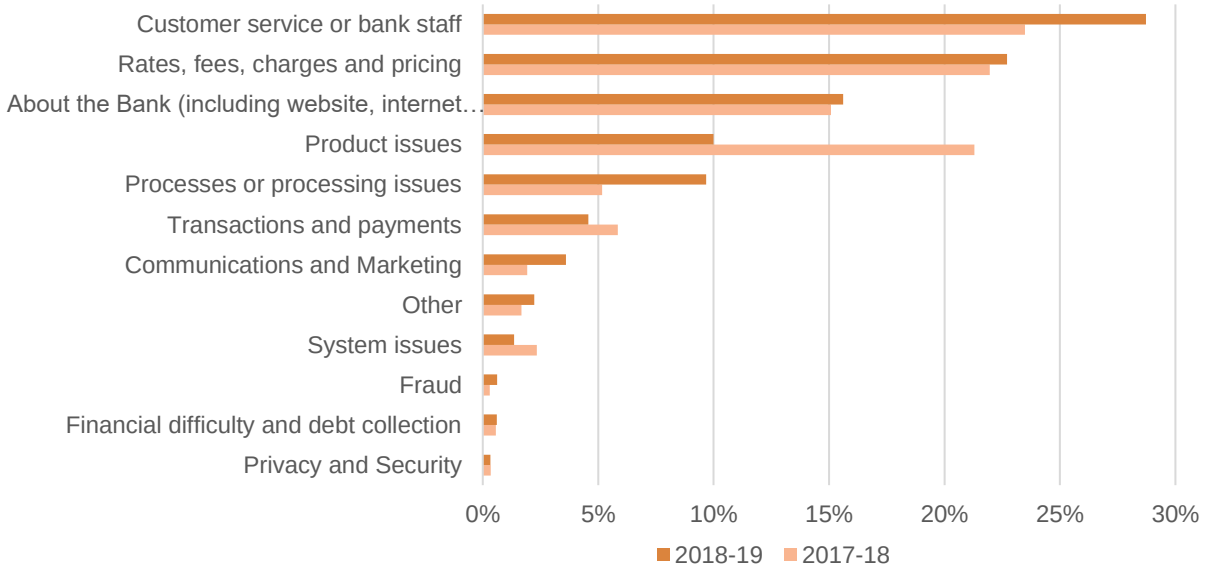
Credit cards (29%) continued to be the top product of concern in 2018–19, consistent with last year.

Chart 10. Complaints received, by product, 2015–16 to 2018–19



Complaints were most commonly about customer service or bank staff (29%) and rates, fees, charges or pricing (23%), consistent with last year.

Chart 11. Complaint Issues, 2018–19



Breach trends

Banks reported 2,432 IDR breaches, a 480% increase from 419 in 2017–18. Seven banks reporting IDR breaches saw an increase this reporting period, with three banks reporting breaches after reporting zero breaches last year.

A big 4 bank which accounted for 91% of IDR breaches, reported an increase of 527% between 2017–18 and 2018–19. The bank explained that the increase in reported IDR breaches was due to an increased focus as a result of ASIC's close and continuous monitoring program and the establishment of a project to address the failure to provide final response letters in all instances.

Table 17. IDR breaches, by bank, 2018–19

Bank	2017–18	2018–19	Change from 2017–18
Big 4	353	2,212	527%
Big 4	30	157	423%
Bank A	9	16	78%
Big 4	10	11	10%
Big 4	13	11	-15%
Bank B	1	10	900%
Bank C	2	7	250%
Bank D	-	3	-
Bank E	-	2	-
Bank F	1	2	100%
Bank G	-	1	-
Total	**419**	**2,432**	**480%**

Following the ACS reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 2,399 IDR reaches – 99% of the total reported. The rest of this chapter refers only to this subset of 2,399 breaches.

The nature and impact of the breaches

Most IDR breaches (66%) were due to a bank's failure to provide a progress update and/or a final response letter within an appropriate timeframe. A big 4 bank reported 1,409 breaches of this type and has implemented several process and system improvements to reduce the likelihood of such breaches recurring.

The next most common breach type, accounting for 33% of the total, occurred when banks failed to register or record a customer's complaint. In these cases, banks addressed these issues by logging the customer's complaint and providing training and coaching to staff members involved.

The remaining breaches occurred where a bank:

- did not send a final response in writing to the customer
- failed to provide an adequate final response letter
- provided customers with incorrect external dispute resolution information, and
- experienced other IDR process issues.

The IDR breaches impacted 4,667 customers in total. One of the breaches where a bank failed to provide an adequate final response letter impacted 2138 customers.

Two banks reported a financial impact for only two breaches amounting to $4,580.

What caused the breaches and how they were identified

Banks reported that 99% of IDR breaches were caused by human error, with the majority of errors identified through call monitoring or quality assurance activities.

How the breaches were corrected

Banks described implementing one or more of the following corrective actions:

- provided staff with further training, coaching or feedback (2,386 breaches)
- corrected the issue such as recording the complaint or sending a final response letter (2,216)
- enhanced monitoring or controls (1,407)
- reviewed processes or made improvements (1,406)

- apologised to the customer (7)
- paid compensation to the customer (1), and
- held performance management discussions with staff (1).

Investigations were ongoing for six breaches, including one which the bank described as a 'significant' breach where final response letters were not sent to customers. The bank has been unable to confirm the number of customers impacted at this point and is working to improve system controls. The matter has been reported to ASIC.

Staff Training and Competency

Clause 9 of the 2013 Code set out standards for staff training and competency.

Breach trends

Banks reported 190 staff training breaches in 2018–19, a 126% increase from the 84 staff training breaches in 2017–18. This figure, however, is closer to the 202 breaches reported in the 2016–17 ACS. This suggests that the 2018–19 figure, despite the rise, may be consistent with longer term trends in breaches of this provision.

Despite reporting no breaches last year, Bank A reported 53 breaches this year, which accounts for much of this increase. The bank advised this is likely due to improvements it made in its Code breach reporting processes. These improvements led to improved staff awareness in identifying and reporting breaches of the 2013 Code. Another big 4 bank saw a significant rise in breaches from six to 26. This bank stated it was unable to identify a clear reason behind the increase.

Overall, ten banks reported breaches of the staff training provisions of the 2013 Code, the highest in three years. Three banks did not report any breaches of this provision. None of these banks have reported a breach in the last three years.

Table 18. Staff Training and Competency breaches, by bank, 2016–17 to 2018–19

Bank	2016–17	2017–18	2018–19
Bank A	34	-	53
Bank B	26	32	30
Big 4	14	19	29
Big 4	-	6	26

Bank	2016–17	2017–18	2018–19
Big 4	4	5	13
Big 4	117	17	12
Bank C	2	-	10
Bank D	-	-	8
Bank E	-	-	5
Bank F	5	5	4
Total	**202**	**84**	**190**

Following the ACS reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 84 staff training breaches – 44% of the total reported. The rest of this chapter refers only to these breaches.

The nature and cause of the breaches

Banks described 72 (86%) staff training and competency breaches as general staff errors. These breaches do not specifically reference training in the description of the incident, but staff did not demonstrate required competency to discharge their functions as required. This is a significant increase on 2017–18 where only 34% of breaches were due to general staff errors. Banks attributed human error to 65% of these breaches. Errors relating to control, training, or resourcing were responsible for the remaining 35%.

The remaining 12 (14%) staff training and competency breaches refer to instances where staff performed their role without completing necessary or mandatory training. While this is a significant percentage decrease from 66% in 2017–18, the number of instances decreased only by ten (22 in 2017–18, 12 in 2018–19). Banks attributed the majority of these breaches to human error (75%).

Small business – Case study

Clause 9 – Staff training and competency

A bank reported a breach of clause 9 of the 2013 Code – Staff training and competency – to the BCCC.

The Code breach related to an incident where a director of a small business was able to transfer $100,000 from the small business company account to his personal account. The staff member failed to check and update the system for any amendments to the signing clause.

The bank reported that the breach was a result of human error and was identified when the small business complained. The bank remediated this breach by refunding $100,000 to the small business account.

The bank also ensured that the relevant staff member and other staff members have undertaken staff training, coaching and feedback to ensure the correct process is followed. The bank has also updated its procedure guide to emphasise the importance of checking signatories on small business accounts.

The impact of the breaches

These detailed breaches affected 2,843 customers, a significant increase from 2017–18 where 106 customers were affected by staff training and competency breaches. The financial impact of these breaches also saw an extraordinary increase from the previous years' figures. The financial impact was $2,422,270 in 2018–19 up from $60,882 in 2017–18.

This significant increase was driven primarily by two big 4 banks, which reported an overall financial impact of $1,436,750 and $780,000 respectively. In the case of the first bank, two breaches contributed to this figure: one breach related to funds being withdrawn contrary to customer instructions; the other breach concerned insufficient information being provided to customers. In the case of the second bank, an incorrect setting up of a payment program led to overcharging fees for 1,921 customers.

How the breaches were corrected

Banks took steps to address privacy and confidentiality breaches which heavily emphasised preventing recurrence. They stated that 83 breaches (99%) included a remediation to prevent recurrence, and 48 (57%) involved action to remediate the customer.

Where banks sought to prevent recurrence, they prioritised staff training and feedback for 71 breaches (85%). Process reviews and improvements were also implemented for nine breaches (11%), and in rare circumstances, staff disciplinary action was taken (4%).

When banks sought to remediate the customer, banks undertook one or more of the following actions:

- individual issue corrected (26 breaches)
- customer refund or reimbursement (25)
- customer apology (8)
- complaint logged and managed (8), and
- communication with the customer or correspondence sent (3).

Terms and Conditions

Clause 12 of the 2013 Code set out banks' obligations to provide customers with terms and conditions, as well as information about fees, insurance options and interest rates.

Breach trends

Banks reported 296 terms and conditions breaches in 2018–19. This is a 48% increase from the 200 reported in 2017–18.

Table 19. Terms and Conditions Breaches, by bank, 2017–18 to 2018–19

Bank	2017-18	2018-19	Change 2018–19
Big 4	103	143	39%
Big 4	14	45	221%
Bank A	1	41	4,000%
Bank B	11	26	136%
Big 4	56	14	-75%
Bank C	-	12	0%
Big 4	2	4	100%
Bank D	5	3	-40%
Bank E	-	3	0%
Bank F	4	3	-25%
Bank G	2	2	0%
Total	**198**	**296**	**48%**

The rise in terms and conditions breaches was driven primarily by three banks. These banks saw breaches increase by 40 (39%), 31 (221%) and 40 (4,000%) respectively.

The Big 4 bank with the highest number of breaches attributed this increase to changes in its branch network. The bank stated that increased monitoring of sales activities in its branches, combined with additional testing of customer outcomes, had led to more breaches being detected. Bank A, which saw a considerable increase, stated it was aware of this rise but could not identify any specific contributing factors. One Big 4 bank saw a 75% drop in its terms and conditions breaches. It accounted for this decline by saying it had in previous years reported breaches that were not appropriate for this provision.

Following the ACS' reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 221 terms and conditions breaches – 75% of the total reported. The rest of this chapter refers only to this subset of 221 breaches.

The nature of the breaches

Most breaches (154, 70%) involved terms and conditions that were issued incorrectly or not at all. Additional breaches concerned terms and conditions not being complied with (37,17%) and terms and conditions containing the wrong information (15, 7%).

Emerging Issue – Clause 12.6

One trend in terms and conditions involved increased numbers of breaches concerning clause 12.6 of the 2013 Code. This required banks to every year remind customers who have a credit facility secured over a primary place of residence or residential investment property of their obligations to insure the property under the terms and conditions of their relevant mortgage. The reminder must also include: a general statement to make inquiries with their insurer about cover; and, a reference to ASIC's MoneySmart website (www.moneysmart.gov.au) for information on property insurance.

During the 2017–18 reporting period, no bank reported a breach of clause 12.6. For the 2018–19 period, five banks reported a breach of clause 12.6. One bank detailed that they had not provided these reminders to customers for over three years. Another bank stated that it had neglected to inform its customers of the ASIC Moneysmart process specifically. Two banks cited the transition to the 2019 Code as the reason that they were able to identify the breach. A further two banks attributed the identification of the breach to increased staff awareness. The number of customers from each bank impacted by the breaches was ranged from 70, with the highest number of customers impacted being approximately 300,000.

The BCCC will continue to monitor this area closely. One particularly notable breach was investigated by the BCCC during the 2018–19 period. The affected bank remediated the issue by contacting and informing its customers of the breach.

What caused the breaches and how were they identified

Human error was the most common cause of terms and conditions breaches (176, 80%), with a control, training or resourcing failure also cited (34, 15%).

Most terms and conditions breaches were at least partially identified through line 1 monitoring or quality assurance processes (150). Other common identification methods included the breach being self-identified by a staff member (39), wider internal review (12) and customer complaint (11).

The Impact of the breaches

In 2018–19, terms and conditions breaches affected 867,891 customers, with a total financial impact of $1,553,682. This is a significant increase from 2017–18 when 128,446 customers were impacted, with a total financial impact of $603,629.

Table 20. Impact of Terms and Conditions breaches, by bank, 2017–18 to 2018–19

Bank	Breaches	Customer Impact	Financial Impact
Big 4	140	2,853	-
Big 4	39	22,048	$730,896.39
Bank A	13	313,031	$3,000.00
Big 4	8	74,323	$5,000.00
Bank B	6	1,096	$800,240.00
Big 4	4	2	-
Bank C	3	162	$882.00
Bank D	3	454,300	$7,485.00
Bank E	3	5	$6,179.00
Bank F	2	71	-
Total	**221**	**867,891**	**$1,553,682.39**

A breach by Bank B had a financial impact of $800,000. The breach was due to terms and conditions being changed which were not then adhered to. This resulted in charging approximately 900 customers a cost that was different to the fees stated in the Terms & Conditions. Bank B has refunded customers and initiated a system fix to address the issue.

How the breaches were corrected

Banks approach to correcting terms and conditions breaches appear comprehensive. Banks took steps to prevent recurrence in its remediation in 215 breaches (97%) and remediated the customer individually in 192 breaches (87%).

To prevent recurrence, banks most often conducted one of the following:

- provided staff training, coaching or feedback (158 breaches)
- process review/ improvements (25)
- enhanced monitoring and controls (16)
- implemented a system fix (11)
- staff performance management (7)

To address customer impact, banks most often conducted one of the following:

- communicated or corresponded with the customer (150 breaches)
- corrected an individual issue (34)
- refunded, reimbursed or otherwise compensated customers (10)

Compliance with Laws

Under clause 4 of the 2013 Code, banks committed to comply with all relevant laws.

The CCMC compliance monitoring functions and powers only extended to clause 4 where a breach of this clause was also a breach of another provision of the 2013 Code. The CCMC previously acknowledged that banks may nevertheless wish to record breaches of clause 4 where they are the primary Code breach, without a link to a corresponding breach of other clauses. The ACS accommodated this approach and consequently some banks – but not all –reported compliance with laws breaches.

Breach trends

Banks reported 476 compliance with laws breaches, a 20% decrease from 594 in 2017–18. This indicates a downward trend in the last three years, with a 25% decrease from 632 in 2016–17. Bank A has traditionally accounted for a significant majority of breaches of Compliance with Laws and this trend continues with the bank reporting 271 (57%) of the 2018–19 breaches. This percentage is down slightly from 2017–18 however, where Bank A reported 68% of total compliance with laws breaches in 2017–18.

The decline in Bank A's absolute number of breaches largely accounts for the overall decrease, and in fact over half of the banks actually reported an increase in Compliance with Law breaches.

Table 21 – Compliance with laws breaches, by banks, 2017–18 and 2018–19

Bank	2017–18	2018–19	Change 2018–19
Bank A	403	271	-33%
Big 4	36	84	133%
Bank B	8	26	225%
Big 4	6	20	233%
Big 4	0	20	0
Bank C	10	17	70%

Bank	2017–18	2018–19	Change 2018–19
Bank D	8	15	88%
Bank E	9	12	33%
Bank F	86	7	-92%
Bank G	7	4	-43%
Bank H	21	0	0
Total	**594**	**476**	**-20%**

Three banks reported no Compliance with Laws breaches. As raised in previous years, due to the broad nature of clause 4, the BCCC expects breaches are likely. Therefore, where banks did not report any clause 4 breaches, the BCCC considers that this is likely a result of a decision not to report these in the ACS, rather than an absence of the underlying conduct.

Following the ACS's reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 183 compliance with laws breaches – 38% of the total reported. The rest of this chapter refers only to this subset of 183 breaches.

The nature of the breaches

The nature of Compliance with Laws breaches was broad. The most common issues included one or more of the following:

- False, misleading or inadequate information provided to customers (35 breaches)
- Payment errors, such as mistaken internet payments, interest or discount errors and overcharging (32)
- Anti-money laundering or know your customer issues (27)
- Delay in remediating customers (16)

What caused the breaches

Most of the Compliance with Laws breaches were caused by human error (95, 52%). Control, training or resourcing error (62) was the second most common cause, followed by system error, failure, issue (20).

How the breaches were identified

Compliance with Laws breaches were identified in a range of ways. Most prominently, they were identified by one or more of line 1 monitoring, system monitoring or other quality assurance work (55 breaches), self-reported by a staff member (45) or complaint or customer query (38).

The impact of the breaches

Compliance with Laws breaches continue to have a large impact, likely due to the range, size and scope of incidents covered by this provision. 3,635,412 people were impacted and the financial impact on customers of these breaches was just under $36 million.

One Big 4 bank accounted for 3,491,870 of the customer impact, though this was spread across several breaches. The largest of this impacted 1,866,000 people and was a breach due to a defect in a template for loan account statements that led to information being left out of customers statements.

Unlike customer impact, the financial impact was more concentrated. A breach by one big 4 bank accounted for $18,000,000 of the financial impact, just over 50% of the total reported. This was the result of certain customers with term deposit accounts receiving an interest rate lower than what was advertised on account opening or renewal. A technical fix has been implemented to address the error, and customer remediation has begun.

Table 22. Impact of Compliance with Laws Breaches, By Bank 2018–19

Bank	Breaches	Customers Impact	Financial Impact
Big 4	61	126,350	$4,934,821.00
Bank A	38	15,917	$782,125.00
Bank B	22	0	$20,559.22
Big 4	20	3,491,870	$21,688,920.00
Big 4	20	9,862	$8,498,940.00
Bank C	12	1,036	-
Bank D	5	3	-
Bank E	2	236	-
Bank F	2	0	$48,926.00
Bank G	1	0	-
Total	**183**	**$3,645,274**	**$35,974,291.22**

How the breaches were corrected

Banks' preference when correcting breaches was to prevent recurrence. Banks stated that on nearly all occasions banks included a step to address recurrence (176, 96%), while a significant majority, though less than for recurrence, included a step to remediate the customer (136 breaches, 74%).

When banks sought to remediate the customer, banks undertook one or more of the following actions:

- individual issue or details corrected (59 breaches)

- customer refund or reimbursement (35), and
- communication with customer (18)

When banks sought to prevent recurrence, they prioritized one or more of the following actions:

- staff training and feedback (79 breaches)
- process review or improvements (50)
- system fix (38), and
- enhanced monitoring or controls (11)

Privacy and Confidentiality

The privacy and confidentiality requirements of the 2013 Code are set out in clause 24.

Breach trends

Banks reported 4,821 breaches of the privacy and confidentiality clause of the 2013 Code in 2018–19, an 8% increase on the 4,464 breaches reported in 2017–18.

In previous years, one large bank has been responsible for a majority of the breaches of this provision, and this remains consistent this year. This bank reported 2,317 breaches, or 49% of the total. However, this is a decrease from 2017–18 – where this bank accounted for 2,767 and 62% of the total.

The decrease in this bank's reported breaches is not representative of other banks' results. Except for one bank, all others reported increases in breaches of privacy and confidentiality.

Table 23. Privacy and confidentiality breaches, by bank, 2017–18 to 2018–19

Bank	2017–18	2018–19	Change 2018–19
Big 4	2,767	2,317	-16%
Big 4	264	579	119%
Big 4	428	475	11%
Big 4	240	386	61%
Bank A	233	356	53%
Bank B	229	335	46%
Bank C	131	169	29%

Bank	2017–18	2018–19	Change 2018–19
Bank D	23	56	243%
Bank E	96	41	-57%
Bank F	20	36	80%
Bank G	18	36	100%
Bank H	15	32	113%
Bank I	0	3	-
Total	**4,464**	**4,821**	**8%**

Several banks provided reasons for why their breach numbers increased. They stated the increase was due to a greater focus on accurate detection and monitoring of privacy and confidentiality breaches within the bank.

Some banks stated that greater education and awareness of frontline staff contributed to lodging more breaches, with one bank citing 50 further breaches being raised from staff awareness than in previous years.

Other banks emphasised tailored monitoring schemes, while one pointed towards the increased sophistication of the risk management practices within the bank.

Following the ACS reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 3,538 privacy and confidentiality breaches, or 74% of the total reported. The rest of this chapter refers only to this subset of 3,538 breaches.

Emerging Issue – Clause 24

Banks are required to report breaches of clause 24, Privacy and Confidentiality.

An emerging trend has been identified where banks have reported that staff members have increasingly sent confidential information or documents to their own personal email address (so that they could work from home, for example) or used their own personal email address for business purposes.

Three incidents of this were reported by three banks in the 2017–18 period. In the 2018–19 period, 38 incidents of this nature were reported by four banks. Banks reported that these 38 incidents affected 219,700 customers.

The BCCC notes that banks could prevent further breaches by reminding staff members of the correct policy or procedure for handling customer information, or sensitive bank information.

Breaches of this nature have been categorised in this Report as “document or information security issues.”

The nature of the breaches

Information provided or disclosed to an incorrect party was the largest breach type identified, accounting for 38% of total breaches. Tax File Number (TFN) issues also contributed to several breaches (23%), followed by privacy policy scripting not read or not disclosed (13%).

Table 24. Types of privacy and confidentiality breaches, 2018–19

Nature of Breach	Breaches	% of breaches
Information provided or disclosed to incorrect party	1344	38%
Tax File Number (TFN) issues	830	23%
Privacy policy scripting not read/ not disclosed	445	13%
Incorrect linking of accounts	200	6%
Document or information security issues	182	5%
Internal privacy policy/procedure not complied with	181	5%
Credit bureau/ reference check issues	131	4%
Documentation/contracts sent electronically without being encrypted/secured	104	3%

Customers experiencing vulnerability – Case study

Clause 34 – Privacy and confidentiality

The breach occurred when a staff member at the bank gave the phone number and address of a co-borrower to the other co-borrower during a phone call. This information should not have been released. A family violence incident occurred because of this privacy breach.

This incident was identified through a complaint made to the FOS (now AFCA). The breach was caused by a failure to follow the bank's processes and procedures.

The bank contacted the affected customer and took steps to ensure the safety of the customer and their children. This included using the bank's security provider, giving the customer a personal duress device and the installation of security systems at the customer's home. In addition to this, the bank has undertaken staff training, coaching and feedback and a review of their processes to prevent these incidents from recurring.

What caused the breaches

An overwhelming majority of privacy and confidentiality breaches (3,374 or 95%) included human error as a cause. A system error, failure or issue accounted in part for 61 breaches, while a control, training or resourcing error accounted for 55 breaches.

How the breaches were identified

The banks reported that 2,538 breaches (72%) were identified at least partially through Line 1 monitoring or quality assurance work. Complaints or customer queries were responsible for identifying a further 803 of the breaches and staff member reporting accounted for 384 breaches.

The impact of the breaches

1,612,601 people were affected by privacy and confidentiality breaches in 2018–19. This is a 253% increase from 2017–18. The financial impact of these breaches was $828,000, a more modest 21% increase from 2017–18.

One breach at one bank affected 400,000 customers. In this instance, personal and financial information was accidentally placed on a share drive available to all bank staff and certain third-party contractors. Once identified, the bank moved to alter access to the files on the drive and investigated the problem. The bank initiated enhanced monitoring and controls and notified relevant customers.

Table 25. Impact of privacy and confidentiality breaches, by bank, 2018–19

Bank	Breaches	Customers Impacted	Financial Impact
Big 4	2,271	153,241	$70,084.00
Big 4	374	387	$7,500.00
Big 4	285	287,056	$340,749.60
Bank A	219	974,271	$157,986.00
Bank B	125	311	$189,110.00
Big 4	75	7,170	$13,044.75
Bank C	66	130	$11,582.00
Bank D	66	200	$38,434.86
Bank E	32	187,215	-
Bank F	12	2,458	-
Bank G	7	157	-
Bank H	3	3	-
Bank I	3	2	-
Total	**3,538**	**1,612,601**	**$828,491.21**

How the breaches were corrected

Banks' steps to address privacy and confidentiality breaches emphasised preventing recurrence. 3,514 breaches (99%) included a commitment to prevent recurrence, whereas 2628 (74%) involved action to remediate the customer.
The main actions to prevent recurrence were implementing one or more of the following corrective actions:

- staff training/ coaching/ feedback (3,527 breaches)
- implementing a consequence, disciplinary action or performance management for the staff member involved (268)
- process improvements or review (103), and
- enhanced monitoring or controls (39).

The main actions to remediate customers were implementing one or more of the following actions:

- corrected the individual issue (1,192 breaches)
- customer apology (888)
- customer refund or reimbursement (577), and
- request that information be destroyed, deleted or returned (430).

Direct Debits

Clause 21 of the 2013 Code required banks to promptly process a customer's request to cancel a direct debit. This is an important and unique protection of the 2013 Code.

Due to the CCMC identifying poor compliance with this provision over a long period, the BCCC takes compliance with this provision very seriously. In the last year, the BCCC has taken targeted steps to monitor compliance with the direct debit provisions and will continue to do so in 2019–20.

Breach trends

Banks reported 224 direct debit breaches, a 30% increase from the 172 reported in 2017–18. This increase has been primarily driven by two Big 4 banks, which reported an increase of 26 and 12 breaches respectively.

Table 26. Direct debit breaches, by bank, 2017–18 to 2018–19

Bank	2017–18	2018–19	Change 2018–19
Big 4	125	151	21%

Bank	2017–18	2018–19	Change 2018–19
Bank A	16	23	44%
Big 4	22	20	-9%
Big 4	2	14	600%
Bank B	2	9	350%
Big 4	-	4	-
Bank C	2	2	0%
Bank D	-	1	-
Bank E	3	0	-100%
Total	**172**	**224**	**30%**

Four banks did not report any breaches of the direct debit provisions of the Code.

Following the ACS reporting instructions (see p. 8), banks provided further information about the nature, cause, impact and correction of 74 direct debit breaches, 33% of the total reported. The rest of this chapter refers only to these breaches.

The nature, cause and impact of the breaches

Banks detailed that a majority of the direct debit breaches (76%) concerned a bank's failure to cancel a direct debit at a customer's request. Customers being provided incorrect direct debit cancellation information accounted for the second highest number of breaches (9%).

Human error was the primary reason provided for the cause of these breaches on 54 occasions (73%). In 18 instances (24%), breaches were either still the subject of ongoing investigation or insufficient information was provided by the bank.

Banks stated the financial impact of these breaches was $48,926 and 69 customers were impacted.

How the breaches were identified and corrected

Direct debit breaches continue to be identified primarily through customer complaints. Banks reported that 73% of breaches were identified in this way, similar to 2017–18 (82%) and 2016–17 (77%).

Line 1 monitoring, system monitoring, or quality assurance accounted for identification of 12 (16%) breaches. A further six breaches (8%) were identified through audit or mystery shopping exercises, including those carried out by the CCMC and passed to the bank as part of its ongoing monitoring work.

Banks' steps to address direct debit breaches were equally distributed between remediating the customer and reviewing processes to prevent recurrence. One or more actions to address customer remediation were reported for 57 breaches (77%), and this number also reflects breaches where process improvements were addressed.

Where banks sought to remediate the customer, they took one or more of the following actions:

- corrected the individual issue or cancelled the direct debit (48 breaches)
- customer apology (19)
- customer refund or reimbursement (19), and
- communication with customer (2).

Where banks sought to prevent recurrence, they used staff training, coaching and feedback in all 57 instances. In one instance, a bank also placed a staff member on a performance management program.

Despite the increased reported breaches in 2018–19, the BCCC remains of the view that these breaches are still likely under-reported in comparison to levels of non-compliance found in the industry. The BCCC's own monitoring conducted during 2018–19, taking place via mystery shopping, found that almost half the interactions with banks revealed non-compliance. The BCCC notes that four banks did not report any breaches of the 2013 Code, despite no banks demonstrating 100% compliance in the mystery shopping exercise.

The BCCC considers the low number of breaches, and the fact they continue to be identified predominately by banks' own customers, an example of our belief that banks place insufficient focus, monitoring and recording on non-compliance with the direct debit provisions.

The BCCC hopes that transition to the 2019 Code will act as a catalyst for change in banks' activities to try and comply with the Code. The BCCC will be monitoring closely to see if this is the case in 2019–20 and the BCCC will act if it has continued concerns banks are not taking this matter seriously.

More details on the BCCC's work on direct debits can be found on the BCCC website.

Updates to breach details since 2017–18

Banks provided details of 7,477 breaches from 2017–18. These breaches had an impact on 3,433,841 customers and had a financial impact of $95,764,211. Of the 7,477 breaches reported by banks in 2017–18, there were 1,354 that were still undergoing investigation at the time of reporting to the CCMC.

The majority (1,046) of these breaches were provision of credit breaches reported by one bank, where supporting documents did not match or support some elements of the credit decision. The bank reported that these files were placed on a watchlist for 12 months. The CCMC followed up with the bank to further understand the impact of the breaches, the outcomes of the 'watchlist' process and what actions were being taken to prevent recurrence.

The bank advised it was undertaking a project to investigate historical compliance dating back several years and covering many more incidents than just those reported in the 2017–18 ACS. The bank confirmed that 8% of the files placed on a watchlist had shown signs of stress such as arrears and requests for financial difficulty assistance. The bank was further investigating these files. The bank confirmed it had delivered numerous training programs and support to its call centre staff to improve practices and several other controls were put in place.

The bank noted that it had identified a reduction in the number of confirmed incidents in 2018–19. However, as above, this bank reported an increased number of provision of credit breaches of this type in 2018–19.

The BCCC asked banks to provide an update on 305 of the remaining breaches when completing the 2018–19 ACS. These breaches included those where banks were still investigating the impact and corrective actions and remediation had yet to be finalised.

Initial reports stated that these breaches impacted 1,334,797 customers and had a financial impact of $75,268,219. The updated details provided by banks now confirm that 1,531,205 customers were impacted, and the total financial impact was $188,170,491. This means that the updated total financial impact of the 2017–18 breaches was $208,666,483 and 3,630,249 customers were impacted.

For 212 of the 305 breaches, banks have provided an update which confirms that appropriate remedial and corrective actions have taken place or that ASIC is monitoring the matter. For four of the 305 breaches reported by banks, the banks have now confirmed that after further review they do not consider a Code breach to have occurred.

There are 89 breaches where the final outcomes is still to be confirmed or insufficient information was provided. The BCCC will continue to liaise with the banks on these as required.

Two other breaches reported separately by another bank now form part of a major ongoing investigation by the BCCC.

End of Report