BANKING CODE COMPLIANCE
MONITORING COMMITTEE

REPORT

Compliance with the Code of Banking Practice 2017–18

Banks' Annual Compliance Statement results

NOVEMBER 2018

Contents

Chair's message

As the Independent Chair of the Banking Code Compliance Monitoring Committee (CCMC), I am pleased to present this report on banks' compliance with the Code of Banking Practice (the Code) in 2017–18. This report sets out the findings from our analysis of banks' responses to the Annual Compliance Statement (ACS), supplemented with information from our subsequent discussions with banks about their responses, held during October 2018.

The report is one outcome of the CCMC's strong focus on enhancing our data collection tools and analysis. The driver for this work was our desire to increase banks' accountability for their compliance with the Code. We want banks to be transparent with the community about the times they let customers down, and about how they identify and address these mistakes.

Monitoring of the Code

This year, banks reported 10,123 Code breaches, a 9.5% reduction on the previous reporting period. The impact of banks' non-compliance with the Code was widespread, affecting at least 3.4 million people at a financial cost of more than $95 million.

In the long term, the CCMC would like to see breaches driven down by improved compliance. At this stage, however, we are not convinced that the decrease in reported breaches reflects improved compliance with the Code.

Rather, we remain concerned about the quality of banks' compliance frameworks and their ability to identify, record and report Code breaches. Lending, collecting debt and resolving customer complaints are core areas of banking activity yet this year, several banks reported zero breaches of the Code's obligations in these areas. Five banks reported zero breaches of the Code's provision of credit and internal dispute resolution obligations, while six banks reported no breaches of their debt collection obligations. This is unlikely to accurately reflect the true situation on the ground.

Some banks continued to report low breach numbers but could not demonstrate compliant processes or robust compliance monitoring processes. These banks gave a range of explanations for low breach numbers. One said that its breaches were immaterial and did not warrant reporting; another acknowledged that while breaches had probably occurred, it could not explain why these had not been reported in its ACS. Such explanations are unacceptable to the CCMC. Where we have concerns about an individual bank's breach reporting, we have begun investigations, examining that bank's conduct and compliance frameworks in more detail.

We also have concerns about the comprehensiveness of banks' Code breach monitoring and reporting. For several years, the data has suggested that banks' compliance efforts are concentrated on those Code provisions that mirror legislative obligations in areas such as provision of credit, internal dispute resolution, debt collection and privacy. Few banks, however, report on breaches of the Code's more nuanced requirements.

Correcting mistakes

We previously highlighted concerns about how banks report corrective actions in our Code breach reporting inquiry. Unfortunately, the 2017–18 ACS highlights the same problem: banks too often fail to report not just on what they have done to stop the breach recurring, but also on how they have remediated those customers affected by the breach.

In some areas, such as the provision of credit, the CCMC is concerned that banks' approach to remediating breaches is not proactive enough. Too often, rather than taking initiative to address an issue, banks rely on account monitoring to identify customers having difficulty repaying. For the most part, compensation is provided to customers only following a directive from the Australian Securities and Investments Commission or an external dispute resolution scheme.

Banks need to do better; they must not rely on individual customers to know and assert their rights. Banks must take steps to understand the extent and impact of the breach and to proactively remediate and compensate customers where it is appropriate.

In June 2018 the CCMC made a clear statement to Code subscribers: when banks do the wrong thing, we expect them to correct their mistakes. This position remains unchanged.

As we move towards implementation of the new Banking Code of Practice, in July 2019, the CCMC will challenge banks to take a more proactive approach to remediating breaches, and to place affected customers at the centre of these efforts.

Looking ahead

The CCMC has much to do as we move towards implementation of the new Code and towards our transition to the Banking Code Compliance Committee. Our preparations for the new Code will begin with a series of roundtable discussions in which we will work with banks to iron out breach reporting inconsistencies and establish a common understanding of the CCMC's expectations of banks under the new Code. Throughout the year, we will also investigate specific compliance issues, and continue our efforts to improve data collection by providing guidance on breach reporting requirements. We will also be following up with banks to track and, where necessary, report publicly on the actions they have taken to address breaches, remediate customers and improve Code compliance.

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

Introduction

This report summarises banks' compliance with the Code of Banking Practice (the Code) in 2017–18. It is based on results from the Annual Compliance Statement (ACS), the main Code compliance monitoring activity conducted each year by the CCMC. The ACS enables the CCMC to benchmark banks' compliance with the Code, report on current and emerging compliance issues, and identify priority areas for future monitoring.

The CCMC

The CCMC is an independent compliance monitoring body established under clause 36 of the Code. The CCMC's purpose is to monitor and drive best practice Code compliance, working collaboratively with the banking sector and other key stakeholders. To achieve this, the CCMC:

- examines banks' practices
- identifies current and emerging industry-wide problems
- recommends improvements to bank practices
- consults with stakeholders and the public and keeps them informed.

The ACS

The ACS seeks information from banks about their compliance with the Code (2013 version) and is the CCMC's major data collection activity. The ACS program is conducted in accordance with clauses 5.1(e) and 5.2 of the CCMC Mandate.

Data collection

This year, the CCMC made major improvements to the ACS, substantially revising the type and breadth of breach data collected. With the 2017–18 ACS, the CCMC has taken an approach similar to that used in the CCMC's recent Breach Reporting Own Motion Inquiry.[1] As a result, this year's ACS is distinctly different to the ACS in previous reporting periods.

For 2017–18, the CCMC asked each Code-subscribing bank to report the total number of Code breaches it identified during the reporting period. Banks were asked to provide further detail about breaches meeting any of the following criteria:

- the bank or any other forum considered the breach of the Code to be significant, systemic or serious
- the breach had an impact on more than one customer
- the breach had a financial impact of more than $1,000 on a customer
- the nature, cause and outcome of more than one breach is the same.

[1] CCMC, June 2018, *Own Motion Inquiry: Breach Reporting*.

In addition, the CCMC asked banks to report details for a random sample of 5% of the remaining breaches of each Code clause. Since significant breaches are included in the new data collection framework, this year the CCMC did not request separate significant breach reports.

Analysis and discussion

After analysing the ACS data, the CCMC provided each bank with a data report benchmarking it against the industry as a whole. In late October 2018, the CCMC met with each bank to discuss this report and the outcomes of the 2017–18 ACS.

The Report

The data in this report is provided on a de-identified basis and banks are not given a consistent label throughout. For example, Bank A in one chart may not be Bank A in another. 'Big 4' is one of the four major banks and other banks are listed as A to J where relevant.

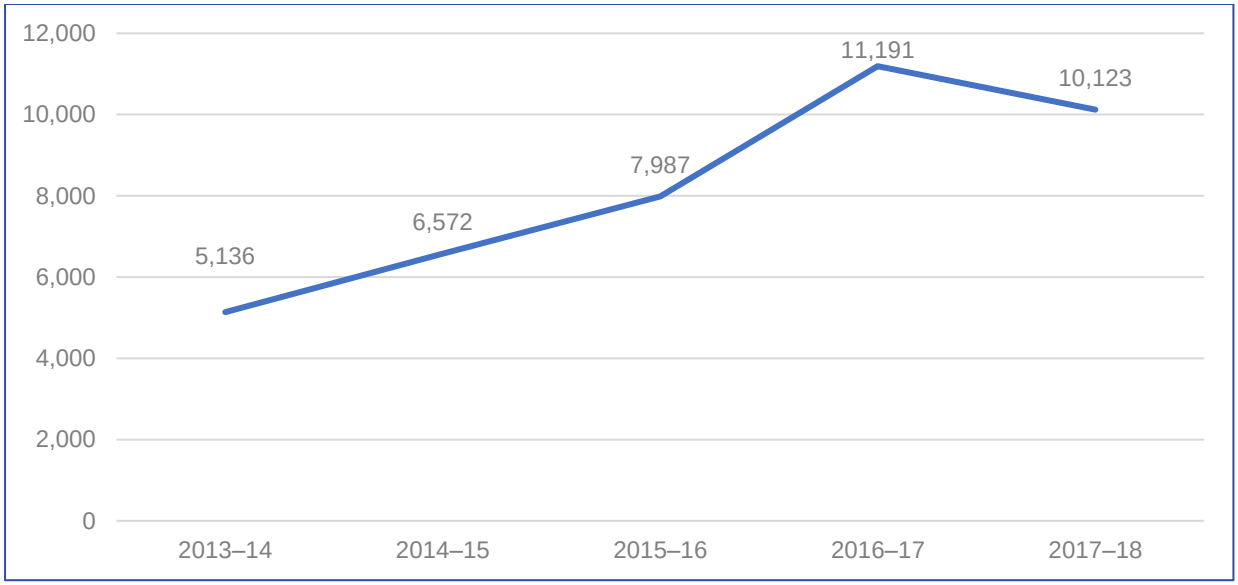
As noted above, banks provided details of a sample of the total number of breaches. As a result, the total figures for some aspects of the data do not match the total number of breaches reported.

Breaches overall

Breach trends

Banks reported 10,123 breaches in 2017–18, a 9.54% decrease from 11,191 in 2016–17 (**Chart 1**).

Chart 1. Code breaches, 2013–14 to 2017–18



The Code clauses that are most commonly breached have remained largely similar over the past five years (**Figure 1**).

Figure 1. Top five Code breach categories, 2013–14 to 2017–18

2013–14	2014–15	2015–16	2016–17	2017–18
24 - Privacy and confidentiality (1,745)	24 - Privacy and confidentiality (1,795)	27 - Provision of credit (2,328)	27 - Provision of credit (4,178)	24 - Privacy and confidentiality (4,464)
04 - Compliance with Laws (757)	27 - Provision of credit (1,318)	24 - Privacy and confidentiality (2,108)	24 - Privacy and confidentiality (2,743)	27 - Provision of credit (2,489)
03 - Key Commitments (739)	04 - Compliance with Laws (1,126)	04 - Compliance with Laws (1,114)	32 - Debt collection (2,061)	32 - Debt collection (725)
27 - Provision of credit (573)	32 - Debt collection (589)	32 - Debt collection (796)	04 - Compliance with Laws (632)	04 - Compliance with Laws (594)
32 - Debt collection (408)	37 - Internal Dispute Resolution (538)	03 - Key Commitments (555)	03 - Key Commitments (472)	37 - Internal Dispute Resolution (419)

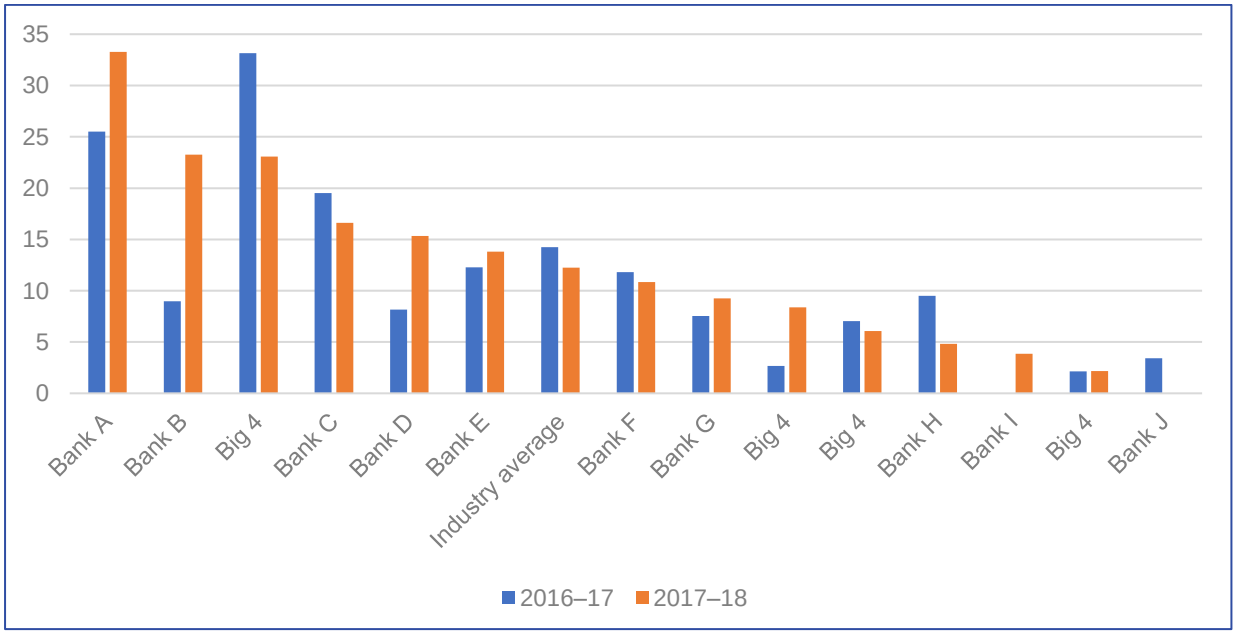
There continues to be wide variation in the number of breaches self-reported by different banks (**Table 1**). Most banks reported an increase in breaches between 2016–17 and 2017–18. However, a large drop in the number of breaches reported by one Big 4 bank led to an overall decrease.

Table 1. Code breaches, by bank, 2013–14 to 2017–18

	2013–14	2014–15	2015–16	2016–17	2017–18	Change 2017-18
Big 4	2,512	3,592	4,832	8,064	5,848	-27%
Big 4	503	309	210	320	1,060	231%
Bank A	672	1,095	975	649	873	35%
Big 4	515	365	912	800	718	-10%
Big 4	227	390	450	420	455	8%
Bank B	33	21	152	168	447	166%
Bank C	21	31	82	240	283	18%
Bank D	37	465	100	146	151	3%
Bank E	28	131	177	258	145	-44%
Bank F	578	147	41	62	58	-6%
Bank G	–	17	24	31	44	42%
Bank H	10	9	31	30	39	30%
Bank I	–	–	–	–	2	–
Bank J	–	–	1	3	–	–
Total	**5,136**	**6,572**	**7,987**	**11,191**	**10,121**	**-10%**

Chart 2 displays banks benchmarked by the number of breaches reported per $1 billion of household deposits[2] for 2016–17 and 2017–18.

Chart 2. Code breaches per $1 billion of household deposits, by bank, 2016–17 and 2017–18



[2] APRA Monthly Banking Statistics for June 2017 and 2018 (www.apra.gov.au)

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 7,477 breaches – 74% of the total reported. The rest of this chapter refers only to this subset of breaches.

What caused the breaches

Asked to comment on the cause of selected breaches, banks reported that the vast majority of breaches (97%) had a single cause. Just 2.4% of breaches had multiple causes. In addition, no cause was reported for 3 breaches, and 35 were still being investigated.

Where a cause or causes were reported:

- 93% involved human error
- 5% involved a control, training or resourcing failure, including process deficiencies
- 2% involved a system error
- 28 breaches involved staff misconduct or fraud.

How the breaches were identified

Almost two-thirds of breaches (65%) were identified through Line 1 quality assurance activities including call monitoring. The other main methods of breach identification were:

- review by the second line of defence (14%)
- customer complaint (9%)
- self-reporting by bank staff (5%)
- internal review (3%).

However, the proportion of breaches identified by a particular method varies enormously across different banks. For example, Line 1 quality assurance accounted for between 1.6% and 77% of identified breaches at different banks. Similarly, complaints led to the identification of as little as 0.3% and as many as 70% of identified breaches. One bank had no breaches self-reported by staff, while staff self-report accounted for some 64% of another bank's breaches.

The impact of the breaches

Banks reported that 7,477 Code breaches in 2017–18 impacted more than three million customers, with a total financial impact of around $95 million (**Table 2**).[3] As banks have not finished investigating all breaches, however, the actual impact may be greater.

Table 2. Impact of Code breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Big 4	4,874	532,169	$ 362,480
Bank A	813	190,196	$ 959,628
Big 4	571	717,789	$ 71,890,106
Big 4	420	483,142	$ 1,847,567
Big 4	277	479,559	$ 11,341,989
Bank B	180	443,946	$ 31,195
Bank C	151	47,622	$ 338,125
Bank D	63	472,410	$ 6,592,590
Bank E	44	7,610	$ 521,498
Bank F	43	2,302	$ 1,251,390
Bank G	30	57,061	$ 624,743
Bank H	9	12	$ -
Bank I	2	23	$ 2,900
Bank J	–	–	–
Total	**7,477**	**3,433,841**	**$ 95,764,211**

Certain types of Code breach are associated with a larger customer impact. For example, although banks reported relatively few breaches of the Code's key commitments obligations, these 243 breaches had the largest impact both in terms of the number of customers affected and the financial impact (**Table 3**).

Table 3. Impact of Code breaches, by Code obligation, 2017–18

Code obligation	Breaches	Customers impacted	Financial impact
Privacy and confidentiality	2,876	465,166	$ 678,656
Provision of credit	1,928	12,649	$ 8,436,790
Debt collection	665	18,214	$ 141,550
Compliance with Laws	538	733,148	$ 9,434,113
Internal Dispute Resolution (IDR)	406	1,203	$ 39,300
Key Commitments	243	1,503,839	$ 74,869,697
Terms and Conditions	170	128,446	$ 603,629
Guarantees	167	3,718	$ 819,331
Financial Difficulty	110	782	$ 69,607
Pre-contractual and new account information	106	621	$ 9,826
Staff training and competency	53	106	$ 60,882
Direct debits	50	52	$ 12,235
Availability of copies of the Code	35	0	$ -
Electronic communications	30	42,660	$ -
Statement of account	19	494,853	$ 147,207
Chargebacks	14	12	$ 11,773
Closure of accounts in credit	13	750	$ 2,864
Cost of credit	10	618	$ 5,500
Operation of accounts	10	11	$ -
Changes to terms and conditions	7	17,122	$ 48,542
Information relating to foreign exchange services	5	5	$ 118
Copies of documents	4	3	$ 500
Joint debtors	3	122	$ 1,500
Account suitability	3	3	$ 2,143
Branch closure protocol	2	8,800	$ -
Payment and instruments	2	2	$ 215,715
Joint accounts and subsidiary cards	2	2	$ 6,021
Bank cheques and inter-bank transfers	2	1	$ 7,712
External Dispute Resolution	1	865	$ -
Account combination	1	65	$ -
Customers with special needs	1	2	$ 139,000
Availability of information about dispute resolution process	1	1	$ -
Total	**7,477**	**3,433,841**	**$ 95,764,211**

How the breaches were corrected

Last year, the CCMC observed that when correcting a breach, banks tended to focus on preventing recurrence – for example, with staff training or coaching – rather than addressing the breach's impact on a particular customer. Similarly, 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 (**Table 4**).

Table 4. Type of corrective action, by bank, 2017–18, by breach and as a percentage of reported breaches

Bank	Both	Remediating customer	Investigations ongoing	Preventing recurrence
Bank A	45 (71%)	3 (5%)	8 (13%)	7 (11%)
Bank B	21 (70%)	1 (3%)	3 (10%)	5 (17%)
Bank C	5 (56%)	1 (11%)	0 (0%)	3 (33%)
Bank D	77 (51%)	31 (21%)	1 (1%)	42 (28%)
Big 4	127 (46%)	38 (14%)	59 (21%)	53 (19%)
Big 4	253 (44%)	74 (13%)	17 (3%)	227 (40%)
Bank E	332 (41%)	128 (16%)	14 (2%)	339 (42%)
Bank F	17 (39%)	4 (9%)	10 (23%)	13 (30%)
Big 4	1,480 (30%)	22 (0%)	1,108 (23%)	2,264 (46%)
Bank G	10 (23%)	19 (44%)	4 (9%)	10 (23%)
Big 4	73 (17%)	16 (4%)	78 (19%)	253 (60%)
Bank H	15 (8%)	93 (52%)	52 (29%)	20 (11%)
Bank I	0 (0%)	1 (50%)	0 (0%)	1 (50%)
Total	**2,455 (33%)**	**431 (6%)**	**1,354 (18%)**	**3,237 (43%)**

To prevent breaches from recurring, banks had:

- provided staff training, coaching or feedback (5,326 breaches)
- reviewed staff performance or taken disciplinary action (1,992)
- reviewed or improved processes (271)
- enhanced monitoring or controls (243)
- implemented a system fix (92).

To address breach impacts on individual customers, banks reported that they had:

- corrected the issue (1,622)
- corrected details (562)
- apologised to the customer (668)
- provided a refund or goodwill payment (304)
- communicated or corresponded with the customer (201)
- requested that information be destroyed, deleted or returned (186)
- logged, managed or resolved a complaint (32)
- released a guarantor or discharged a mortgage (4).

Banks also reported that investigations were ongoing for 1,354 breaches, and that 15 breaches had been referred to the statutory regulator.

Provision of credit

Banks must 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. These obligations are set out in clause 27 of the Code.

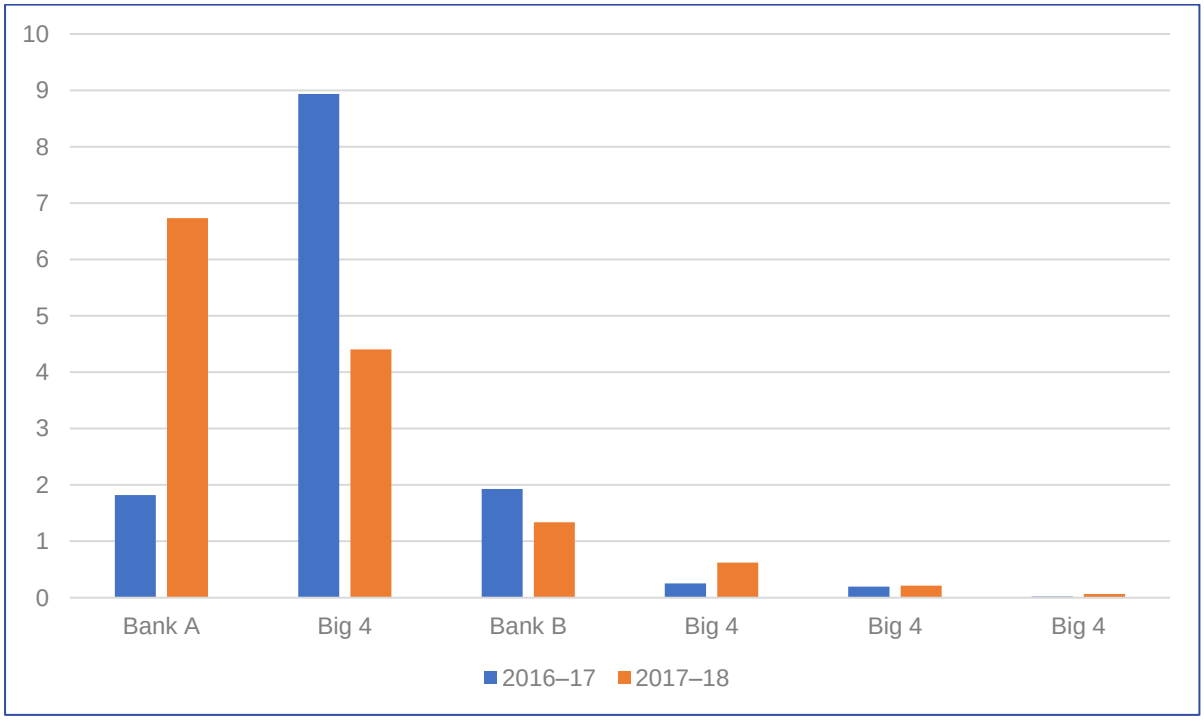
Breach trends

Banks reported 2,489 provision of credit breaches in 2017–18. As in previous years, one outlier bank reported most of these breaches – 1,981 breaches or 80% of the total. Five banks did not report any provision of credit breaches for 2017–18, while three banks each reported only 1 or 2 breaches.

Provision of credit breaches decreased by 40% in 2017–18, falling from a total of 4,178 breaches in 2016–17. The overall decrease this reporting period was largely the result of a 49% drop in breaches reported by one major bank. Bank B (**Chart 3**) that reported a 29% breach decrease, attributed this to renewed compliance efforts, including a focus on ongoing training for lenders; improvements to capacity to repay calculators; and clearer procedures on the information to be used assessing customer loans.

Chart 3 displays banks benchmarked by the number of provision of credit breaches reported per $1 billion of household credit[4] for 2016–17 and 2017–18. It excludes banks that reported two or fewer provision of credit breaches in 2017–18.

Chart 3. Provision of credit breaches per $1 billion of household credit, by bank, 2016–17 and 2017–18



[4] APRA Monthly Banking Statistics for June 2017 and 2018 (www.apra.gov.au)

Against the overall downwards trend, four banks reported an increase in provision of credit breaches in 2017–18 (**Table 5**). Two of these attributed the increases to improvements in monitoring and identification, rather than an actual increase in breaches. Bank A explained that branch managers were now providing in-branch reviews of active and funded loan files, while a dedicated team was performing hindsight reviews of settled loans. The Big 4 bank that saw a 154% increase, said that it had begun capturing and recording breaches identified in monthly assurance reviews at a more granular level.

Table 5. Increase in provision of credit breaches, by bank, 2016–17 to 2017–18

Bank	2016–17	2017–18	Increase 2017–18
Bank A	50	185	270%
Big 4	69	175	154%
Big 4	52	58	12%
Big 4	9	29	222%

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 1,928 provision of credit breaches – 77% of the total provision of credit breaches reported. The rest of this report chapter refers only to this subset of 1,928 breaches.

The nature of the breaches

Most provision of credit breaches reflected three specific issues unique to the Big 4 bank that reported the majority of breaches: supporting documents, telephone information requests and debt consolidation discussions. Together, these three issues account for 1,714 or 69% of the 2017–18 provision of credit breaches. Similar issues also made up most provision of credit breaches in 2016–17.[5]

Supporting documents

The most common issue, accounting for 1,046 breaches in 2017–18, occurred where supporting documents did not match or support some elements of the credit application – most commonly an application for a home loan (762 breaches) or personal loan (204 breaches). The bank also reported 859 breaches of this type in 2016–17.

The bank's credit quality assurance team identified the breaches, which were caused by human error when staff failed to follow the bank's process. Staff were given coaching and performance management and files were placed on a watchlist for 12 months. The CCMC will discuss this matter with the bank and follow up on the impact of the 2016–17 breaches, which have now completed their 12-month watchlist period.

[5] CCMC, June 2018, *Own Motion Inquiry: Breach Reporting*.

Telephone information requests

Another 492 provision of credit breaches occurred where a staff member failed to collect all required information about the customer during the telephone credit application process. The bank explained that its credit application scripts for frontline staff are designed to comply with responsible lending obligations, Code requirements and the bank's internal credit policy. The bank's call monitoring program identifies deviations from the script and, taking a conservative approach, the bank has recorded these as breaches.

In 2016–17, the bank reported more than five times as many breaches of this type (2,577). In 2017, the bank began contacting customers promptly after the identification of a potential issue and before credit was provided. By obtaining any missing information and, where required, reassessing the application, the bank rectified many potential issues. This led to the dramatic drop in breaches of this type this year, and explains most of the overall decrease in banks' provision of credit breaches for 2017–18.

Debt consolidation discussions

Finally, the failure to conduct debt consolidation discussions correctly caused 176 breaches, down from 415 in 2016–17. Both the telephone information request and debt consolidation discussion breaches were caused by human error, when staff failed to follow the process. The breaches were identified through call monitoring and corrected with staff coaching and performance management.

The bank reported, as it did in 2016–17, that these breaches did not have any financial impact on customers. However, the CCMC continues to be concerned by this broad assessment and will follow up with the bank to ensure that any impacts on individual customers has been fully investigated.

Other issues

A range of other issues accounted for the 214 remaining provision of credit breaches for which banks provided additional information. In 191 cases, the lending decision was inappropriate, incorrect or 'not responsible' for one or more of the following reasons:

- the customer's financial situation was incorrectly calculated or recorded (73 breaches)
- the customer could not afford the credit repayments (64)
- the credit application or assessment process was not followed correctly (32)
- the information provided by the customer was not verified or not verified correctly (22)
- a credit check was not completed or completed incorrectly (18)
- a customer was provided with a business loan when it should have been a consumer loan (15)
- the bank used incorrect or incomplete information in its lending decision (9)
- the customer's situation was inappropriate for the credit provided, including for reasons related to age, health or financial situation (7)
- the bank did not make sufficient enquiries about the customer's needs or financial situation (7)
- the credit application was submitted without the customer's permission (2).

Other provision of credit issues included:

- incorrect information provided to customer and loan subsequently not approved (4)
- record keeping issue with the record of the discussion with customer (2)
- processing issues (2)
- customer allowed to overdraw a facility without credit approval (1)
- duplicate credit card issued for a single application (1)
- fraud or misconduct (1)
- inadequate provision of information about fees (1)
- incorrect assessment of customer's borrowing capacity which led to financial loss (1)
- incorrect information provided to customer which led to financial loss (1)
- interest rate error (1).

In addition, there were eight breaches for which the bank did not provide enough information about why the incident was a breach.

What caused the breaches

The overwhelming majority (1,893 or 98%) of provision of credit breaches[6] were caused, at least in part, by human error. Some 16 breaches were caused by a control, training or resourcing failure such as inadequate training or a deficient process. System issues caused 14 breaches and two were caused by staff misconduct or fraud. For another 11 breaches, the banks' investigations were ongoing or the response was insufficient to understand the cause.

How the breaches were identified

The vast majority (96%) of provision of credit breaches[7] were identified through Line 2 or Line 1 monitoring, which accounted for 1,049 and 809 breaches respectively. Breaches were also identified by:

- customer complaint or query (23)
- Financial Ombudsman Service[8] (FOS) (19)
- self-identified or reported by a staff member (17)
- a third party, supplier or collections agency (4)
- internal review (2)
- external event (1)
- internal audit (1)
- a regulator (1)

One major bank did not report how two breaches were identified.

[6] For which details were provided. See note on p. 5.
[7] For which details were provided. See note on p. 5.
[8] The Financial Ombudsman Service (FOS) was replaced by the Australian Financial Complaints Authority (AFCA) on 1 November 2018.

The impact of the breaches

When assessing compliance with a particular Code obligation, the CCMC considers the impact of breaches, not only the number. More than 12,000 customers were affected by banks' provision of credit breaches in 2017–18, with a combined financial impact of over $8.4 million (**Table 6**).

Table 6. Impact of provision of credit breaches, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Big 4	1,733	1,966	$ 194,459
Big 4	80	5,387	$ 786,377
Bank A	51	51	$ -
Big 4	27	361	$ 5,454,793
Bank B	17	21	$ 1,251,170
Big 4	17	4,719	$ 717,721
Bank C	2	143	$ -
Bank D	1	1	$ 32,271
Total	**1,928**	**12,649**	**$ 8,436,790**

While some breaches affect only a single customer, the impact is often much wider. For example, a single systemic breach reported by a major bank impacted 1,205 customers. Due to a transaction processing error (a human error), consumer loan applications failed to prepopulate the customers' asset and liabilities position. This meant that in some cases, the repayment amount of existing loans was not included in the loan serviceability assessment. The bank stated that a system change is needed to fix the issue. As the bank's investigation is continuing, the total financial impact on customers is not yet known. The CCMC will follow up with the bank to understand the full impact and to ensure the issue is fixed and customers are remediated.

Another major bank reported two breaches that together impacted 4,700 customers. Some 4,200 customers were affected by duplicate credit cards being issued to a customer for a single application. The breach was identified by a staff member. Investigations are ongoing, but the bank reported that the financial impact was $250,000. Staff now check within systems if an account is created before proceeding with re-approval. The second breach impacted 500 customers. The bank stated that living expenses were not accurately included in serviceability calculations for overdrafts. The breach was identified by the bank's second line of defence and while remediation was still pending at the time of reporting, the financial impact was $225,000.

A third major bank reported a breach that affected 320 customers, with a total financial impact of around $5 million – accounting for most of the total financial impact of provision of credit breaches. An ASIC investigation found that this breach occurred when the bank failed to take reasonable steps to verify the income figures in 12 motor vehicle finance applications introduced by third party intermediaries, even though it had reason to doubt the reliability of the information. The bank no longer accepts consumer credit applications from the intermediaries involved, and addressed the detriment with a remediation program developed in consultation with ASIC.

Bank B reported six breaches with a combined $1.25 million financial impact. Each breach concerned irresponsible home loan lending. Five of the six breaches were identified by FOS and one was found by internal audit. In each case the debt was reduced or waived, however, the bank did not report any action to prevent similar human error breaches from occurring again.

The 1,714 breaches reported by the major bank and discussed above, impacted a relatively modest 1,953 customers, although at this stage the bank has not reported any financial impact from the breaches.

How the breaches were corrected

Banks reported a range of steps to correct the breaches, but tended to place a heavier emphasis on preventing recurrence than on remediating affected customers (**Table 7**).

Table 7. Types of corrective action for provision of credit breaches, by bank, 2017–18

Bank	Investigations ongoing	Preventing recurrence	Remediating customer	Both
Big 4	1,053 (61%)	674 (39%)	5 (0%)	1 (0%)
Big 4	31 (39%)	17 (21%)	6 (8%)	26 (33%)
Bank A	51 (100%)			
Big 4	2 (7%)		23 (85%)	2 (7%)
Bank B	1 (6%)	8 (47%)	8 (47%)	
Big 4	2 (12%)	1 (6%)	9 (53%)	5 (29%)
Bank C		1 (50%)	1 (50%)	
Bank D	1 (100%)			
Total	**1,141 (59%)**	**701 (36%)**	**52 (3%)**	**34 (2%)**

The specific steps most commonly taken to prevent recurrence were:

- providing staff with further training, coaching or feedback (724 breaches)
- holding performance management or disciplinary discussions with staff members (674)
- reviewing or improving processes (23)
- enhancing monitoring or putting controls in place (8)
- implementing a system fix (2)

Banks addressed customer impacts by:

- refunding, reimbursing or otherwise compensating customers (57)
- communicating or corresponding with the customer (19)
- correcting the issue (15)
- apologising to the customer (1)
- discharge the mortgage over the property and release the guarantees (1)

For 1,141 breaches, banks indicated that their investigations were ongoing, although some specific corrective actions may still have been taken.

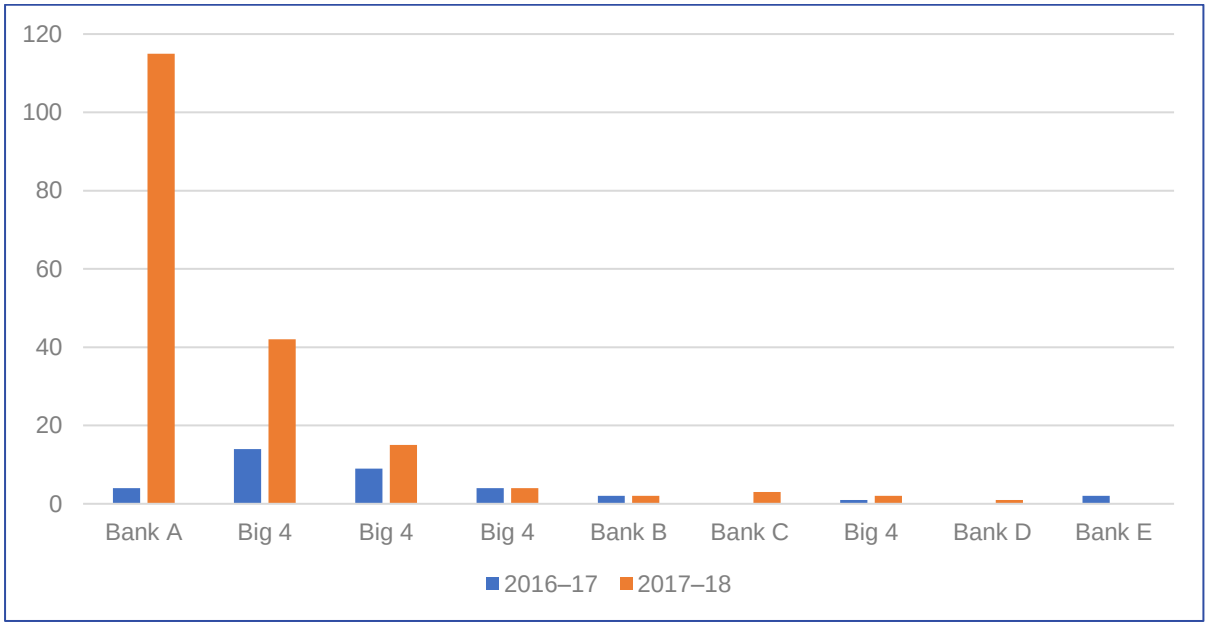
Guarantees

The guarantee obligations under clause 31 of the Code include 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). Banks should allow a potential guarantor until the next day to consider the information provided. The Code also sets out obligations relating to how the guarantee is signed and how guarantors can withdraw from a guarantee.

Breach trends

Banks reported 184 guarantees breaches, a 411% increase from 36 breaches reported in 2016–17. The growth in guarantees breaches can be attributed largely to two banks. Bank A's guarantees breaches rose from 4 to 115 (**Chart 4**). Bank A attributed this enormous 2,775% increase to improved compliance recording, including more hindsight reviews and new error detection controls that require loan processing staff to verify guarantee documents before settling loans. A major bank's breaches increased by 200% from 14 to 42, but offered no explanation for this increase. Another major bank reported a 67% increase from 9 to 15 breaches. In contrast, six banks reported zero guarantees breaches in 2017–18.

Chart 4. Guarantees breaches, by bank, 2017–18



Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 167 guarantees breaches – 91% of the total guarantees breaches reported. The rest of this report chapter refers only to this subset of 167 breaches.

The nature of the breaches

Most guarantees breaches (128, or 77% of the breaches for which details were provided) involved a failure to provide the required disclosures or prominent notices to a potential guarantor. This included Bank A's 109 reported breaches, that occurred when the bank's business banking area failed to provide guarantor disclosures. The bank has addressed the issue through staff training and awareness, however, the bank has not advised the CCMC about the standing of the guarantees for the 191 customers impacted.

In addition, 34 breaches (20%) were related to the execution of the guarantee. This category included instances of guarantees being fraudulently signed as well as cases where guarantee documentation was not witnessed correctly.

What caused the breaches

Process issues, including a deficiency in the process or a lack of understanding of the process, caused 117 (70%) guarantees breaches. A further 50 breaches were due to human error.

How the breaches were identified

Most guarantees breaches were identified through Line 1 quality assurance activities (**Table 8**).

Table 8. Identification of guarantees breaches, 2017–18

Identification method	Breaches	Percentage of breaches
Line 1 monitoring such as quality assurance reviews or call monitoring	155	93%
Self-reported by staff member	8	5%
Customer complaint or query	2	1%
External event	1	1%
FOS	1	1%
Total	**167**	

The impact of the breaches

The 167 breaches for which details were provided impacted at least 3,718 customers (**Table 9**). The vast majority of affected customers were impacted by a single guarantees breach in which Bank C failed to send guarantors all required information about the credit assessment conducted on the borrower. At the time of reporting, Bank C estimated that 3,500 customers were impacted. The CCMC has an ongoing investigation to establish the nature and impact of the breach, and to discuss remediation steps with the bank. The bank classes the breach as significant and has also notified ASIC.

Table 9. Impact of guarantees breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Bank A	115	199	$ -
Big 4	32	1	$ 819,331
Big 4	11	11	$ -
Big 4	3	3	$ -
Big 4	2	1	$ -
Bank B	2	2	$ -
Bank C	1	3,500	$ -
Bank D	1	1	$ -
Total	**167**	**3,718**	**$ 819,331**

This data, however, is incomplete, and probably understates the customer and financial impact of guarantees breaches. A major bank did not report on the number of customers impacted for 32 of its guarantees breaches. That bank was the only bank to provide any information about financial impact – and included this data for four breaches only. Some breaches were still under investigation at the time of reporting, and a lack of financial impact information is acceptable in those cases.

The CCMC believes 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 have told the CCMC that when assessing financial impact, they have not considered any additional fees or costs associated with entering into a flawed guarantee. The CCMC will discuss this with banks to ensure a consistent approach to reporting this information is implemented in future.

How the breaches were corrected

Banks steps to address guarantees breaches emphasised preventing recurrence (**Table 10**). The main actions included:

- providing further staff training, coaching or feedback (144)
- implementing a 'consequence', disciplinary action or performance management for the staff member involved (12)
- implementing system fixes and reviewing or improving processes (6).

Banks addressed individual customer impacts for only 7 breaches, taking action to correct the issue (4 breaches) and releasing the guarantor from the guarantee or not enforcing the guarantee (3). Banks do not appear to have heeded the CCMC's previous advice to reflect the standing of a guarantee when correcting and reporting on a breach.[9] The CCMC's next major own motion inquiry will focus on the Code's guarantees obligations.

[9] CCMC, June 2018, *Own Motion Inquiry: Breach Reporting*.

Table 10. Type of corrective action for guarantees breaches, by bank, 2017–18

Bank	Preventing recurrence	Both	Investigations ongoing	Remediating customer
Bank A	114 (99%)	1 (1%)		
Big 4	31 (97%)	1 (3%)		
Big 4	9 (82%)			2 (18%)
Big 4	2 (67%)			1 (33%)
Bank B			2 (100%)	
Big 4		1 (50%)	1 (50%)	
Bank C		1 (100%)		
Bank D			1 (100%)	
Total	**156 (93%)**	**4 (2%)**	**4 (2%)**	**3 (2%)**

Debt collection

The Code's debt collection obligations are set out in clause 32 and state:

- 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 725 debt collection breaches, a 65% decrease from in 2016-17. Seven banks did not report any breaches of the debt collection obligations.

As with previous years, there is one outlier bank who has reported the majority (476 or 66%) of debt collection breaches. This bank has detailed decreases in breaches from 2016-17 (by 1,494 or 76%). This bank states that the significant reduction in breaches came as the result of process changes. Most debt collection breaches reported by this bank relate to poor quality file notes for collection activity. A process change has concentrated on correcting the file notes as soon as an exception is identified, through call monitoring and prior to any further collections contact with the debtor. In these cases, the breach is negated, and this reduction has been reflected in breach numbers.

The second largest reporter of breaches, another major bank, reported 206 debt collection breaches. This was an increase of 190 breaches since 2016-17. The bank stated that this rise came from further scrutiny of debt collection by quality assurance. This resulted in debt collection data that is often reported internally on a consolidated level, due to the what the bank perceived the minor nature of the breaches, being comprehensively reported for the first time.

Two other banks provided an explanation for their decrease in debt collection breaches. Bank A (**Table 11**) stated that this was due to a recategorisation of how it classifies code breaches. Bank C stated that staff conducted greater inquiries into relevant data to identify whether incidents were in fact breaches.

Of note in this area is the distinction between the largest banks. Two major banks have significantly more breaches of clause 32 than rivals of similar size in the “Big 4”. In addition, according to APRA data, Bank A’s percentage of Australian household credit is less than 5% of that of a major bank that reported one more breach. It should be noted that one major bank in 2016–17 had breach figures broadly in line with two other major banks, until further scrutiny (as detailed above), resulted in an acknowledgment of far greater number of breaches of this obligation.

Table 11. Debt collection breaches by bank, 2016–17 and 2017–18

Bank	2016-17	2017-18	Change 2017-18
Big 4	1,970	476	-76%
Big 4	16	206	1,188%
Big 4	10	17	70%
Bank A	47	16	-66%
Bank B	11	6	-45%
Big 4	1	3	200%
Bank C	6	1	-83%
Total	**2,061**	**725**	**-65%**

Following the CCMC’s reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 665 debt collection breaches – 92% of the total debt collection breaches reported. The rest of this report chapter refers only to this subset of 665 breaches.

The nature of the breaches

Incomplete or inaccurate file notes was the main breach type, accounting for 63% of debt collection breaches. The provision of incorrect information, including the misrepresentation of consequences, accounted for 23% of debt collection breaches (**Table 12**).

Table 12. Debt collection breaches by type, 2017–18

Type of Incident	Breaches	Percentage of breaches
Incomplete or inaccurate file notes	417	63%
Incorrect information, including the misrepresentation of consequences	155	23%
Frequency of contact guidelines not met	27	4%
Debt collection activity during a financial difficulty arrangement or request	21	3%
Improper collections activity	15	2%
Other	30	4%
Total	**665**	

What caused the breaches

An overwhelming majority (630 or 95%) of debt collection breaches were caused by human error. A system error, failure or issue accounted for 19 breaches, while a control, training or resourcing failure contributed 11 breaches.

How the breaches were identified

Most debt collection breaches (587 or 88%) were identified through Line 1 quality assurance and call monitoring. Customers and staff members also contributed, with customer complaints or queries and staff member reporting accounting for 34 (5%) and 30 (5%) breaches respectively. Some 20 debt collection breaches, or 3% of the total, were identified partly through the work of FOS (now AFCA).

The impact of the breaches

Industry reported that some 18,214 customers were impacted by debt collection breaches in 2017–18. The financial impact on customers of these industry breaches stands at $141,550.

Table 13. Impact of debt collection breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Big 4	444	8,000	$ -
Big 4	186	349	$ 140,300
Bank A	16	9,191	$ 1,250
Big 4	11	499	$ -
Bank B	4	11	$ -
Big 4	3	161	$ -
Bank C	1	3	$ -
Total	**665**	**18,214**	**$ 141,550**

Data on the impact of debt collection breaches is incomplete. Although the bank that reported most of the total debt collection breaches and estimated that 8,000 customers were affected, the bank did not identify any financial impact. It reported that it is still investigating the financial impact of many of the breaches it reported.

How the breaches were corrected

Once again, banks' corrective action targeted prevention of future breaches, with little emphasis on remediating affected customers (**Table 14**). To prevent recurrence, banks:

- provided staff training, coaching or feedback (615)
- enhanced monitoring and controls (11)
- implemented a system fix (11)
- reviewing or improving processes (5).

To address customer impacts, banks:

- corrected or updated details (337)
- apologised to the customer (18)
- corrected the individual issue (13)
- communicated with affected customers (9)
- refunded, reimbursed or otherwise compensating customers (7).

Investigation was ongoing for 27 breaches.

Table 14. Type of corrective action for each debt collection breach, by bank, 2017–18

Bank	Both	Preventing recurrence	Investigations ongoing	Remediating customer
Big 4	338 (76%)	83 (19%)	23 (5%)	
Big 4	17 (9%)	164 (88%)		5 (3%)
Bank A		14 (88%)		2 (13%)
Big 4	5 (45%)	1 (9%)	4 (36%)	1 (9%)
Bank B	2 (50%)	2 (50%)		
Big 4	3 (100%)			
Bank C				1 (100%)
Total	**365 (55%)**	**264 (40%)**	**27 (4%)**	**9 (1%)**

Financial difficulty

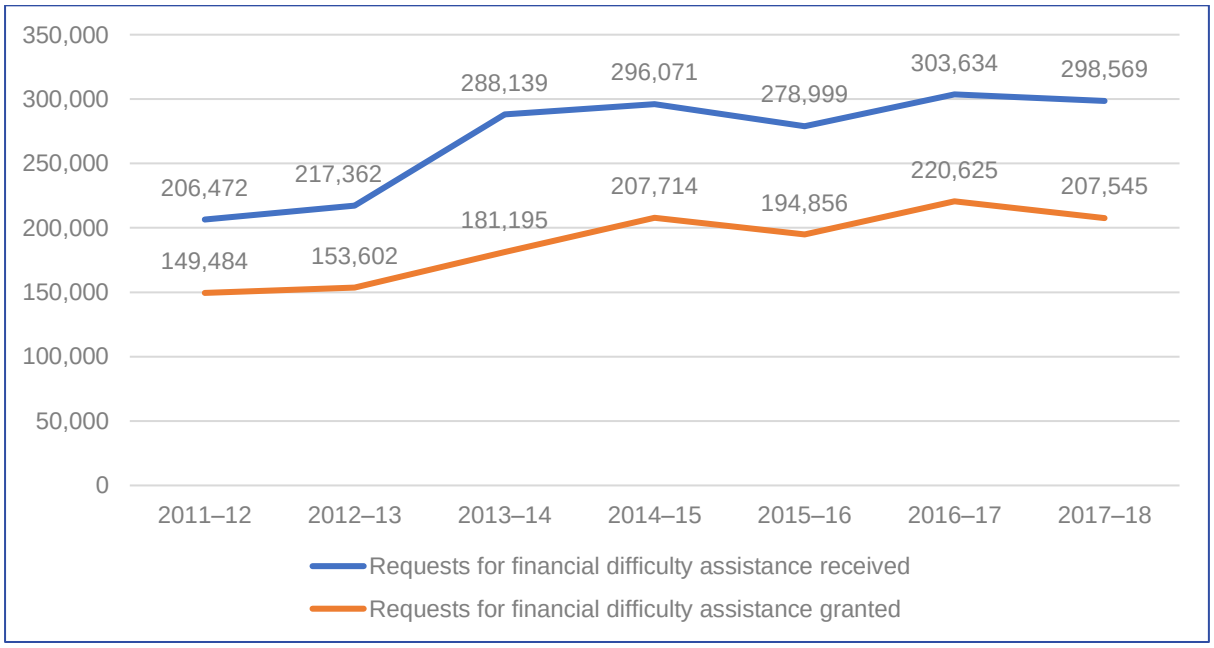
Banks' financial difficulty obligations are set out in clause 28 of the Code. The Code states that banks must try to help customers overcome their financial difficulties with any credit facility they have with their bank.

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 298,569 requests for financial difficulty assistance in 2017–18, a 1.6% decrease from 303,634 requests in 2016–17 (**Chart 5**). Seven banks reported decreases – ranging from 4% to 30% – while six banks saw the number of requests for assistance rise.

Chart 5. Requests for financial difficulty assistance received and granted, 2011–12 to 2017–18



Banks granted assistance on 207,545 occasions – an overall assistance rate of 69.5% (**Table 15**). This is a slight drop from 72.7% in 2016–17, but is broadly in line with the proportion of requests granted since 2011–12.

Table 15. Percentage of requests for financial difficulty assistance granted, 2011–12 to 2017–18

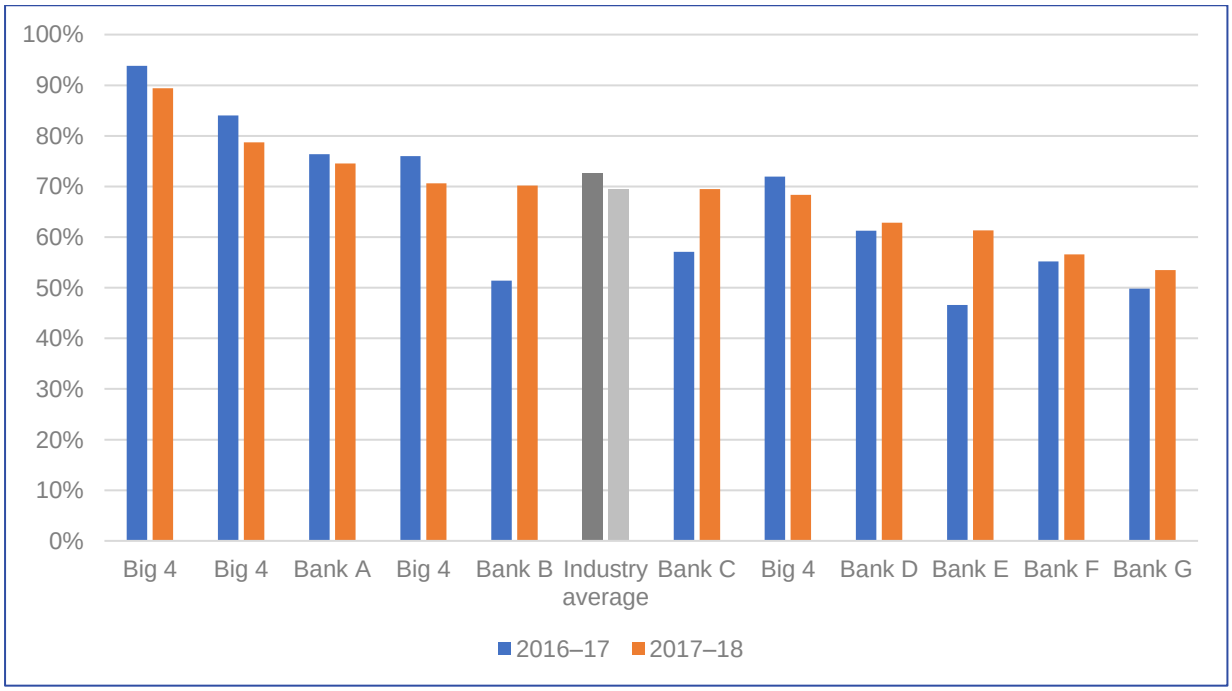
2011–12	2012–13	2013–14	2014–15	2015–16	2016–17	2017–18
72.4%	70.7%	62.9%	70.2%	69.8%	72.7%	69.5%

There is substantial variation between banks in terms of both the number of requests for assistance received and the rate of assistance granted (**Table 16**). However, the divergence between banks' assistance rates decreased in 2017–18, as banks that had the highest and lowest assistance rates in 2016–17 moved closer to the average (**Chart 6**).

Table 16. Requests for financial difficulty assistance received and granted, by bank, 2017–18

Bank	Requests for financial difficulty assistance **received**	Requests for financial difficulty assistance **granted**
Big 4	121,565	83,122
Bank A	48,401	25,894
Big 4	37,124	29,229
Big 4	37,030	26,162
Big 4	28,884	25,818
Bank B	7,727	5,759
Bank C	7,639	4,685
Bank D	4,389	3,049
Bank E	2,591	1,628
Bank F	2,247	1,577
Bank G	799	452
Bank H	165	163
Bank I	8	7
Bank J	0	0
Total	**298,569**	**207,545**

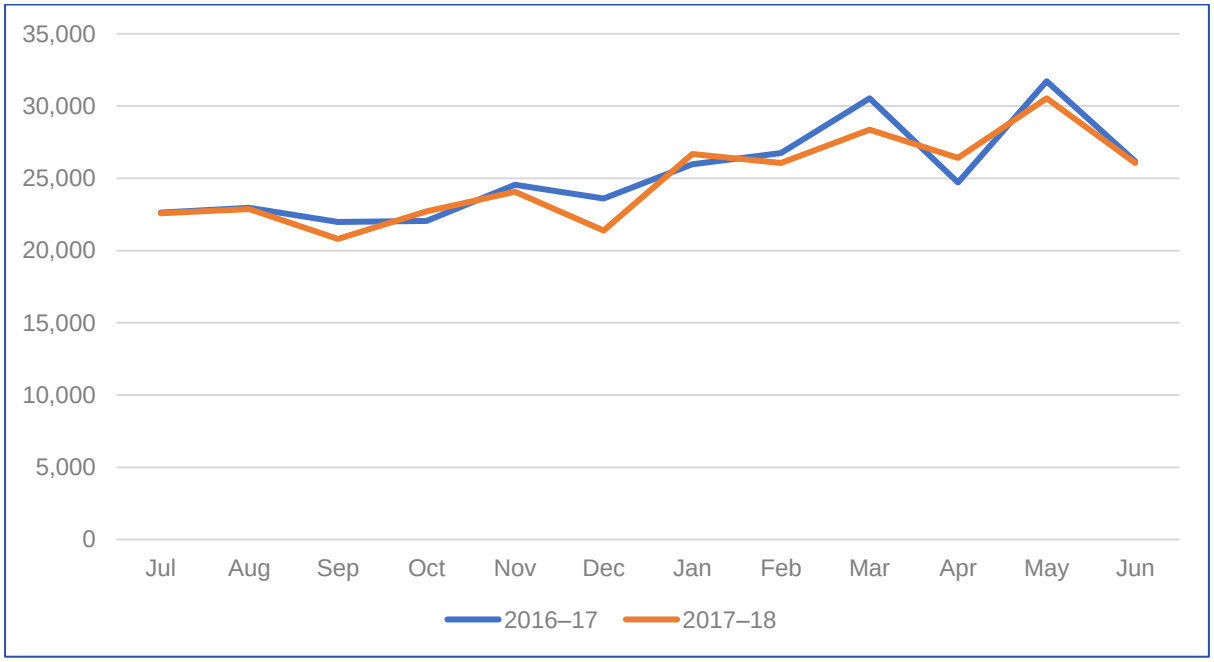
Chart 6. Percentage of requests for financial difficulty assistance granted, by banks*, 2016–17 and 2017–18



* Excludes banks that received fewer than 200 requests for assistance.

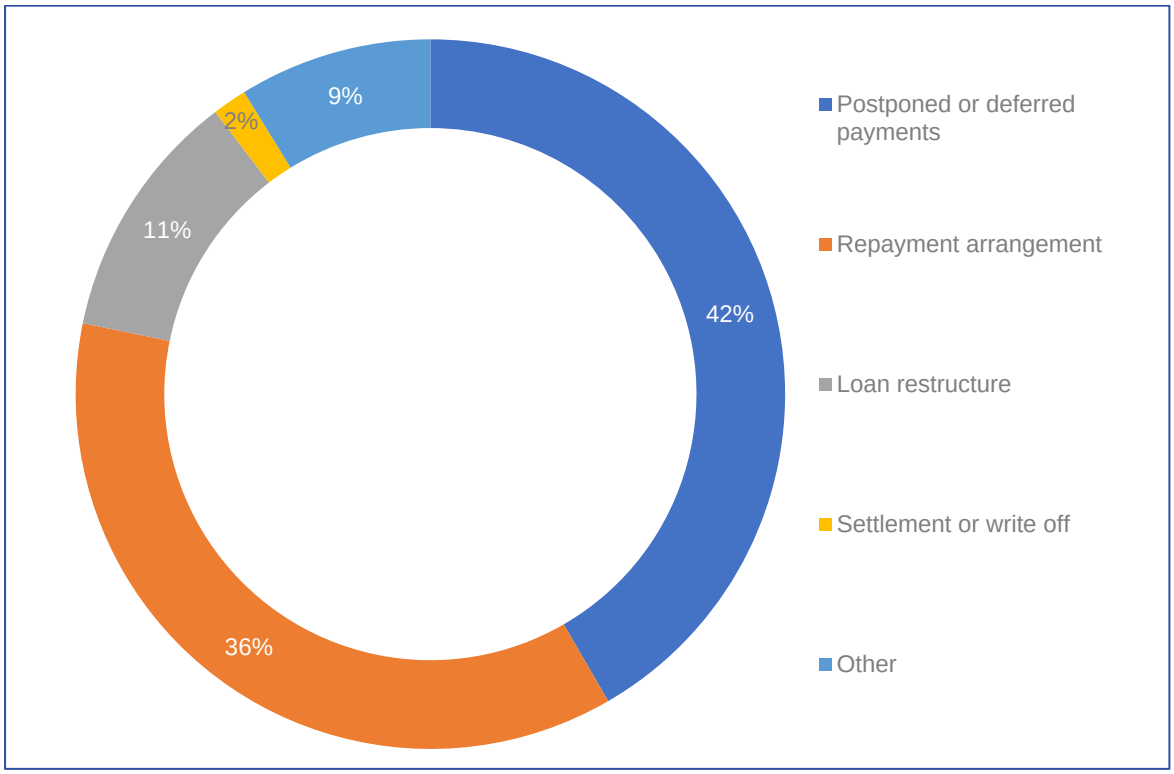
Chart 7 displays the total number of requests for assistance received by month for 2016–17 and 2017–18. The trend is broadly similar for these two reporting periods and indicates that the number of requests received, tends to be higher and fluctuates from month to month towards the end of the financial year.

Chart 7. Requests for financial difficulty assistance received, by month, 2016–17 and 2017–18



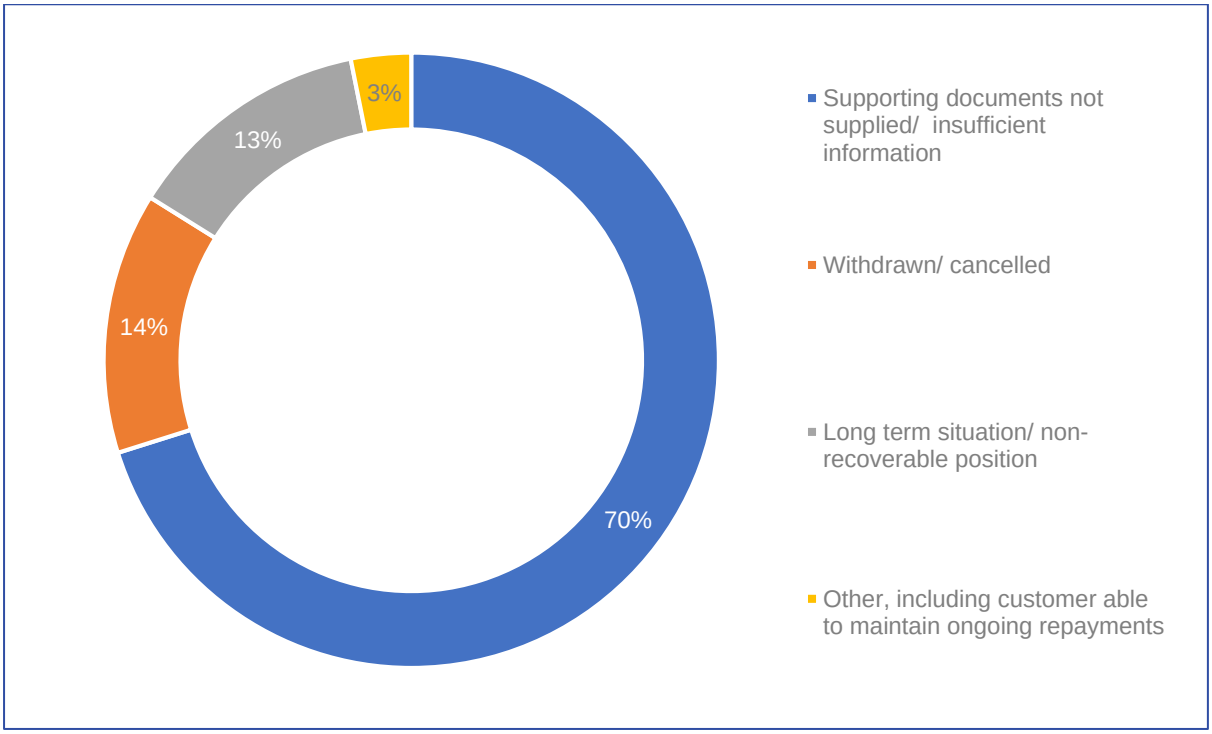
The most common forms of financial difficulty assistance granted by banks in 2017–18 were postponed or deferred payments (42%) and repayment arrangements (36.6%) (**Chart 8**).

Chart 8. Types financial difficulty assistance provided, 2017–18



When banks did not provide financial difficulty assistance, this was most often because the customer did not supply supporting information (70%) or withdrew the application (14%) (**Chart 9**). This aligns with the CCMC's analysis in previous years, however, it should be noted that this data is incomplete. Some banks – including a major bank, which declined more requests than any other bank – did not provide data on the reasons requests were declined.

Chart 9. Reasons financial difficulty assistance was not provided, 2017–18



Breach trends

Banks reported 164 financial difficulty breaches in 2017–18, a 10% decrease from 183 in 2016–17 (**Table 17**). This overall decrease can largely be attributed to a 46% drop in breaches reported by a major bank, from 95 breaches in 2016–17 to 51 in 2017–18. Nevertheless, this bank continued to account for more breaches than any other bank. Four other banks also reported a decrease in financial difficulty breaches.

Five banks reported increased financial difficulty breaches in 2017–18. Only one bank, Bank F, provided an explanation for the increase, attributing it to increased quality assurance activity and better oversight of complaints data.

Table 17. Financial difficulty breaches, 2016–17 to 2017–18

Bank	2016–17	2017–18	Change 2017–18
Big 4	95	51	-46%
Big 4	23	31	35%
Big 4	10	27	170%
Bank A	10	16	60%
Bank B	12	12	0%

Bank	2016–17	2017–18	Change 2017–18
Bank C	10	4	-60%
Bank D	8	6	-25%
Bank E	6	7	17%
Big 4	7	6	-14%
Bank F	2	4	100%
Total	**183**	**164**	**-10%**

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 110 financial difficulty breaches – 67% of the total financial difficulty breaches reported. The rest of this report chapter refers only to this subset of 110 breaches.

The nature of the breaches

The largest contributor to financial difficulty breaches, accounting for 43% of the total, was the failure to action a request for assistance, or to do this within the required timeframe. A further 25% of breaches occurred when a bank did not identify or follow up financial difficulty indicators.

Table 18. Types of financial difficulty breach, 2017–18

Issue	Breaches	Percentage of breaches
Financial difficulty assistance requests not actioned or responded to within timeframe	47	43%
Potential financial difficulty indicators not identified or followed up	27	25%
Financial difficulty arrangements not properly explained to customer	12	11%
Financial difficulty assistance requests not processed correctly or genuinely considered	12	11%
Process errors	6	5%
Other	6	5%
Total	**110**	

What caused the breaches

Most financial difficulty breaches (94 or 85%) were caused, at least in part, by human error. After this, system errors, failures or issues accounted in part for 11 breaches (10%).

How the breaches were identified

Over half of the financial difficulty breaches (62 or 56%) were identified, at least in part, through quality assurance and call monitoring. Bank staff reported a further 12 breaches (11%). Sources outside the bank also played an important role in the identification of financial difficulty breaches: 31 breaches (28%) were identified via customer complaints or queries and/or FOS.

The impact of the breaches

Banks reported that 782 customers were impacted by financial difficulty breaches. Although Bank C reported only 5 breaches, these affected 291 customers, accounting for 37% of the total customer impact of financial difficulty breaches. Some 253 customers were affected by a single Bank C breach when a change to the financial difficulty system introduced an undetected error. Some customers were not sent written requests for information and were consequently denied assistance for failing to provide information in the required timeframe. Bank C addressed the breach by reissuing all relevant letters and offering assistance to those affected. Most customers were contacted and received financial difficulty assistance, and 11 accounts that had been default listed as a result of the breach had the listings removed. However, some customers were uncontactable and two had declared bankruptcy.

The financial impact on customers of these industry breaches stands at $69,607, with 99.7% of this amount reported by just two banks (a major bank and Bank G). While one major bank states it is still investigating financial impact on a number of its breaches, the remaining six banks did not report any financial impact. This includes Bank C, which claims none of the 291 customers affected by its 5 breaches suffered any financial detriment. This claim warrants further evidence and the CCMC will follow up with Bank C.

Table 19. Impact of financial difficulty breaches, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Big 4	37	135	$ -
Big 4	25	40	$ -
Big 4	13	14	$ 45,336
Bank A	12	24	$ -
Bank B	6	7	$ -
Bank C	5	291	$ -
Big 4	4	254	$ -
Bank D	4	3	$ 24,051
Bank E	3	11	$ -
Bank F	1	3	$ 220
Total	**110**	**782**	**$ 69,607**

How the breaches were corrected

In correcting financial difficulty breaches, banks placed fairly equal emphasis on preventing recurrence and addressing the impact on individual customers (**Table 20**). To prevent recurrence, banks most commonly:

- provided staff training, coaching or feedback (50)
- reviewed or made improvements to processes (30)
- enhanced monitoring and controls (4)
- implemented a system fix (4).

To address customer impacts, banks:

- logged and resolved a complaint (27)
- corrected an individual issue (25)

- refunded, reimbursed or compensated the customer (17)
- communicated or corresponded with the customer (15).

Table 20. Type of corrective action for each financial difficulty breach, by bank, 2017–18

Bank	Both	Preventing recurrence	Remediating customer	Investigations ongoing
Big 4	25 (68%)	11 (30%)		1 (3%)
Big 4	25 (100%)			
Big 4	1 (8%)		12 (92%)	
Bank A		11 (92%)	1 (8%)	
Bank B	5 (83%)		1 (17%)	
Bank C	3 (60%)	1 (20%)	1 (20%)	
Big 4	4 (100%)			
Bank D	2 (50%)	1 (25%)	1 (25%)	
Bank E			2 (67%)	1 (33%)
Bank F			1 (100%)	
Total	**65 (59%)**	**24 (22%)**	**19 (17%)**	**2 (2%)**

Banks indicated that no action had been taken on two breaches where investigations were ongoing or no action was required.

Key commitments

Clause 3 of the Code sets out banks' 'key commitments', a set of general requirements concerned largely with how banks will communicate with and inform customers. The CCMC's compliance monitoring functions and powers, however, only extend to clause 3 where a breach of it is also a breach of another provision of the Code.

The CCMC has acknowledged that banks may nevertheless wish to record breaches of clause 3 where they 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.

Breach trends

Banks reported 301 key commitments breaches in 2017–18, an 36% decrease from 472 in 2016–17.

Table 21. Key commitments breaches, by bank, 2016–17 to 2017–18

Bank	2016–17	2017–18	Change 2017–18
Big 4	250	60	-76%
Big 4	147	61	-59%
Big 4	23	55	139%
Bank A	31	27	-13%
Bank B	3	51	1,600%
Bank C	3	16	433%
Bank D		16	
Bank E	1	11	1,000%
Big 4	11		-100%
Bank F	2	2	
Bank G		2	
Bank H	1		-100%
Total	**472**	**301**	**-36%**

Although key commitments breaches decreased overall, a number of banks reported an increase. The largest increase – from 3 to 51 breaches – was reported by Bank B, which provided no explanation for the jump. Three banks attributed increased breaches to breach identification and reporting improvements. For example, Bank D advised that when staff do not follow internal processes and, as a result, fail to act in the spirit of the Code, this is now considered a breach. A major bank said that it now captures breaches identified from monthly assurance reviews on a more granular level.

Similarly, banks that reported decreased key commitments breaches attributed this to interpretation and reporting changes. A major bank said that it had reviewed its breach categorisation, developing an internally consistent approach and communicating this to staff. Another major bank also attributed its decrease to its decision to review and change what constitutes a breach of this clause. All explanations for increases and decreases appear to be due to banks' interpretation and categorisation of the clause. The CCMC will explore this with the banks concerned.

Four banks (including one major bank) did not report any key commitments breaches. In the case of larger banks, this probably reflects a decision not to report breaches of this broad obligation. While this is permitted under the Code, the CCMC will discuss the issue with banks as key commitments breaches may have a major customer and financial impact.

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 243 key commitments breaches – 81% of the total reported. The rest of this report chapter refers only to this subset of 243 breaches.

The nature of the breaches

Key commitments breaches reflected a wide range of issues, namely:

- failure to act on instructions or account processing issues by staff (112 breaches)
- provision of information to customers (61)
- system or process errors (46)
- staff misconduct (11)
- CCI sales practices (8)
- inappropriate provision of credit (5).

The impact of the breaches

The 243 breaches for which details were provided affected at least 1.5 million customers with a financial impact of nearly $75 million (**Table 22**). Two breaches by a major bank accounted for most of this impact. Systems and process error breaches had the greatest impact, affecting 935,746 customers with a financial impact of more than $70 million (**Table 23).**

Table 22. Impact of key commitments breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact	
Big 4	61	379,771	$	5,218,368
Bank A	45	531	$	200,813
Big 4	43	3,218	$	5,320
Big 4	35	712,071	$	66,202,355
Bank B	27	389,886	$	2,876,449
Bank C	16	15,231	$	-
Bank D	11	3,106	$	363,493
Bank E	2	1	$	-
Bank F	2	23	$	2,900
Bank G	1	1	$	-
Total	**243**	**1,503,839**	**$**	**74,869,697**

Table 23. Impact of key commitments breaches, by breach type, 2017–18

Type of incident	Breaches	Customers impacted	Financial impact	
Staff failed to act on instructions or account processing issues by staff	112	89,060	$	1,231,176
Provision of information to customers	61	474,990	$	604,919
System or process errors	46	935,746	$	72,808,132
Staff misconduct	11	2,710	$	16,000
CCI sales practices	8	1,327	$	5,320
Inappropriate provision of credit	5	6	$	204,150
Total	**243**	**1,503,839**	**$**	**74,869,697**

Table 24 provides the details of key commitments breaches that impacted 10,000 or more customers.

Table 24. Key commitments breaches that impacted 10,000 or more customers, 2017–18

Type of incident	Description of incident	Cause	ID method	Corrective actions	Customers impacted	Financial impact	Other comments
System or process error	Loan accounts not closed after full repayment	System error, failure, issue	Control or operational testing	Ongoing investigation Customer refunds	405,404	$ 31,500,000	Significant and reported to ASIC
Provision of information	Correspondence or documentation to customer included incorrect information	Human error	Self-identified or reported by staff member	Staff training, coaching or feedback Communication with customer	255,000	$ -	Significant
Provision of information	Issues with guarantees disclosures	Control, training or resourcing failure	Internal review	Ongoing investigation	150,000	$ -	
System or process error	Cards reissued incorrectly	System error, failure, issue	Customer complaint or query	Ongoing investigation Customer reimbursement	142,270	$ -	Significant and reported to ASIC
System or process error	Incorrect interest rate applied to savings account	System error, failure, issue	Customer complaint or query	Payments to customers and system fix	134,614	$ 2,017,592	Significant and reported to ASIC
System or process error	System wrote off credits rather refunding customer	System error, failure, issue	Self-identified or reported by staff member	Ongoing investigation Refunds to be provided System fix	114,000	$ 350,000	Reported to ASIC
Staff failed to act on instructions or account processing issues by staff	Customers not provided with relevant rewards	Human error	Self-identified or reported by staff member	Points credited to customers	78,000	$ -	

Type of incident	Description of incident	Cause	ID method	Corrective actions	Customers impacted	Financial impact	Other comments
Provision of information	Issues with guarantees disclosures	Control, training or resourcing failure	Internal review	Ongoing investigation	48,000		
System or process error	Home loan and commercial lending accounts not receiving the full benefit of offset arrangements	System error, failure, issue	System monitoring	Ongoing investigation	37,300	$ 8,900,000	Significant and reported to ASIC
System or process error	Customers not provided with relevant discounts and overcharged interest	Control, training or resourcing failure	Control or operational testing	Ongoing investigation	30,700	$ 25,500,000	Significant and reported to ASIC
System or process error	Credit card transactions processed after card closed due to fraud	Control, training or resourcing failure	Self-identified or reported by staff member	Ongoing investigation	30,000	$ 4,000,000	
System or process error	Discrepancy between system actions and PDS disclosures; accounts made dormant too early	System error, failure, issue	FOS	System fix	13,890	$ -	No customer financial impact as these accounts have been inactive for 24 months and classified as dormant
Provision of information	Digital brochures not updated to reflect new information	Human error	Self-identified or reported by staff member	Correct links to information	10,000	$ -	
System or process error	Benefits not applied	Control, training or resourcing failure	Self-identified or reported by staff member	Ongoing investigation	10,000	$ 30,000	

What caused the breaches

Most key commitments breaches were caused by human error (69%). Control, training or resourcing failures including process deficiencies caused 16% of breaches, and systems issues caused 12%.

How the breaches were identified

Customer complaints and queries, rather than banks internal monitoring mechanisms, were the top source of identified breaches.

Table 25. Identification method, key commitments breaches, 2017–18

Identification method	Breaches	Percentage of breaches
Customer complaint or query	86	35%
Staff self-report	52	21%
Line 1 quality assurance monitoring	42	17%
Internal review	20	8%
Internal audit	19	8%
FOS	13	5%
Control or operational testing	4	2%
Third party	2	1%
System monitoring	2	1%
Whistleblower	1	0.4%
Other	1	0.4%
Regulator	1	0.4%
Total	**243**	

How the breaches were corrected

Banks reported a range of steps to correct key commitments breaches, both to prevent recurrence and address customers' individual issues (**Table 26**). To prevent recurrence, banks:

- provided staff with further training, coaching or feedback (41 breaches)
- implemented a system fix (28)
- held performance management or disciplinary discussions with staff members (21)
- enhanced monitoring or put controls in place (20)
- reviewed or improved processes (17).

To address customer impacts, banks:

- refunded, reimbursed or otherwise compensated customers (86)
- corrected the issue (56)
- apologised to the customer (38)
- communicated or corresponded with the customer (17).

There were 98 breaches still under investigation.

Table 26. Type of corrective action for key commitments breaches, by bank, 2017–18

Bank	Investigations ongoing	Both	Remediating customer	Preventing recurrence
Big 4	42 (98%)			1 (2%)
Big 4	35 (57%)	16 (26%)	3 (5%)	7 (11%)
Big 4	12 (34%)	7 (20%)	13 (37%)	3 (9%)
Bank A	4 (15%)	22 (81%)	1 (4%)	
Bank B	3 (7%)	4 (9%)	35 (78%)	3 (7%)
Bank C	1 (9%)	9 (82%)		1 (9%)
Bank D	1 (6%)			15 (94%)
Bank E			1 (50%)	1 (50%)
Bank F			1 (50%)	1 (50%)
Bank G		1 (100%)		
Total	**98 (40%)**	**59 (24%)**	**54 (22%)**	**32 (13%)**

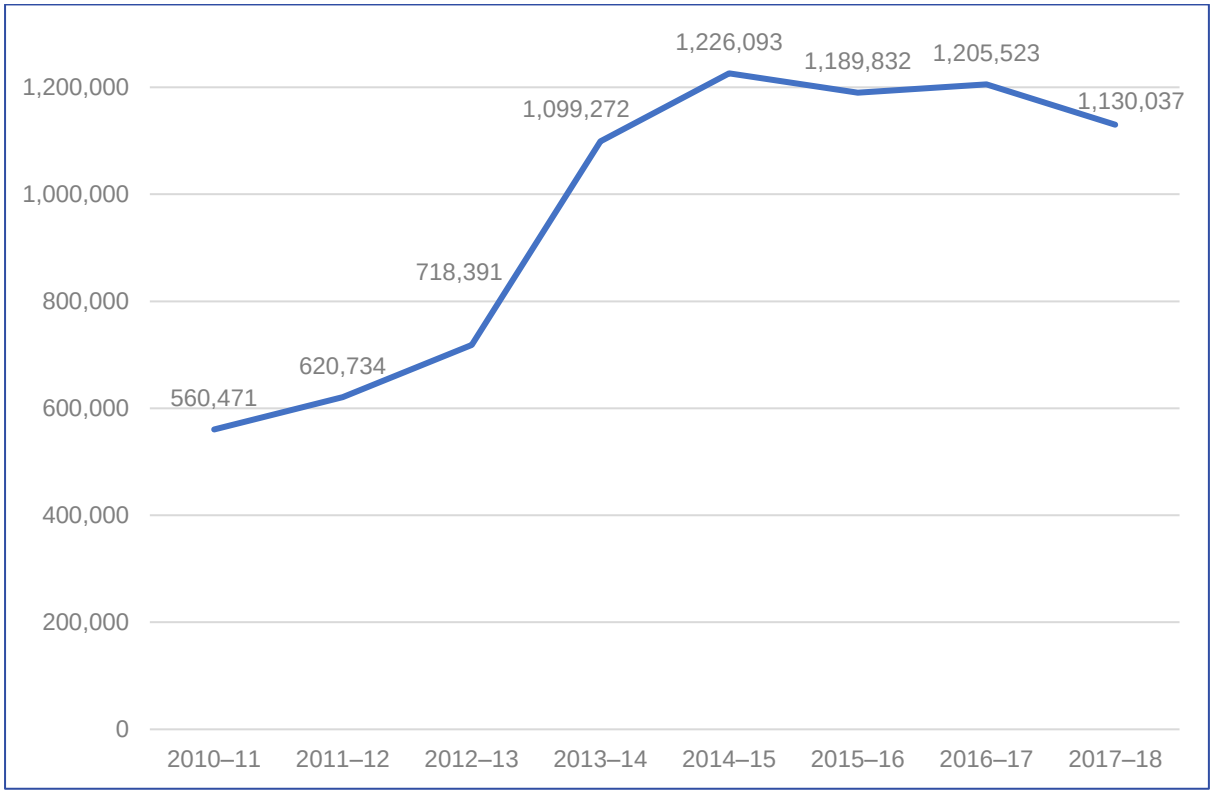
Internal Dispute Resolution

The Internal Dispute Resolution (IDR) obligations under clause 37 of the Code stipulate that banks must have an internal dispute handling process that is free and accessible. The process must meet the standards set out in ASIC Regulatory Guide (RG) 165.

Customer complaints

Banks resolved 1,130,037 complaints in 2017–18, a 6.3% decrease from the 1,205,523 complaints resolved in 2016–17 (**Chart 10**). One major bank makes up most complaints – 68% of the total in 2017–18. This bank's 13% decrease in complaints between 2016–17 and 2017–18 largely accounts for the overall complaints decrease over the same period. Four additional banks reported a decrease, while complaints increased for nine banks, and there was one new Code subscriber.

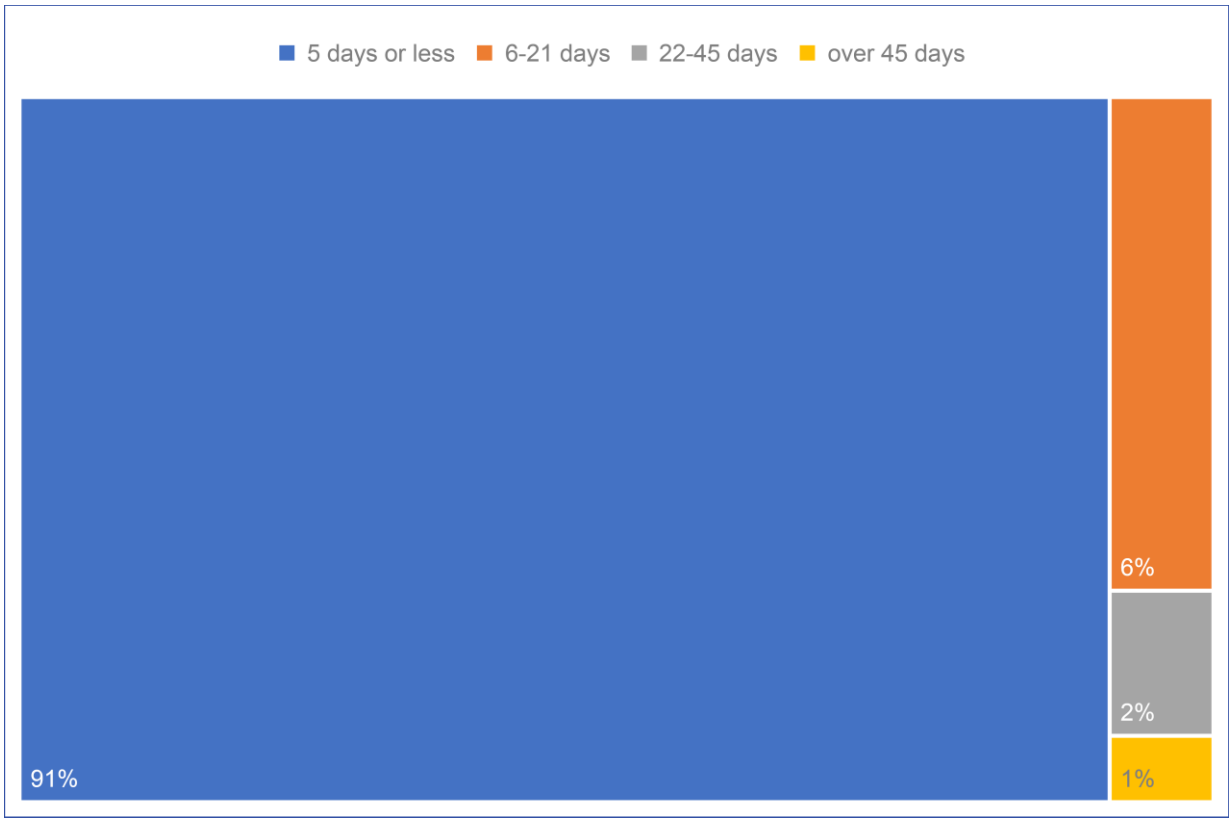
Chart 10. Complaints resolved, 2010–11 to 2017–18



How quickly complaints were resolved

Banks resolved 91% of all complaints within 5 working days (**Chart 11**), a very slight decrease from 92% in 2016–17.

Chart 11. Complaint resolution timeframes, 2017–18



ASIC's RG165 permits banks not to record complaints that are resolved to the customer's complete satisfaction within five business days. This has led to divergent reporting approaches. Some banks capture and report all expressions of dissatisfaction received, regardless of how the complaint is received, the time taken to resolve it or 'where a response or resolution is explicitly or implicitly expected'. Other banks only report complaints that are not resolved immediately and require follow-up.

While both approaches meet the standard set out under RG165, the variation does create inconsistencies in complaint resolution data. Eleven banks stated that their policy is to record all expressions of dissatisfaction, however, two of these reported that this is not always occurring, and that they are investigating improvements. Two banks confirmed that staff are not required to record expressions of dissatisfaction that are resolved at the first point of contact. One bank did not explain its reporting approach.

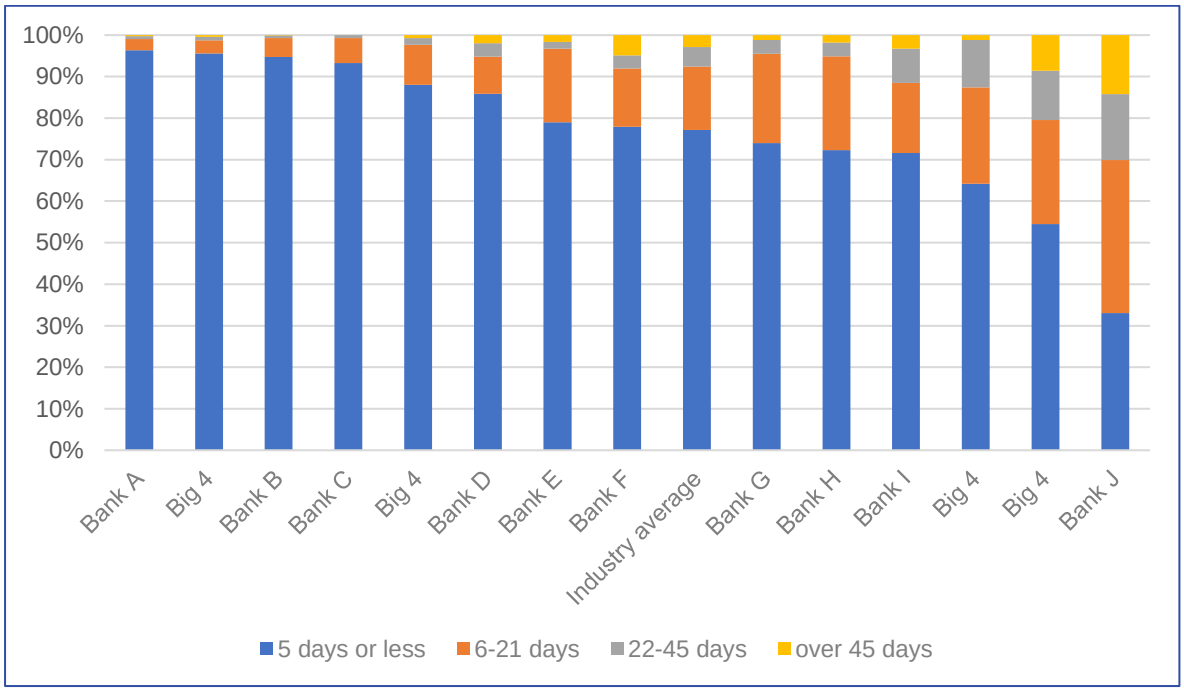
There also appears to be inconsistency in how banks interpret 'expression of dissatisfaction'. Although most banks categorise all expressions of dissatisfaction as a complaint, some banks record some such expressions as 'feedback' or 'suggestions', consequently excluding these from the data provided to the CCMC.

Although RG 165 does not define 'complete satisfaction', banks generally interpret this in the same way. Banks reported that the customer needs to actively confirm, either verbally or in writing, that they are satisfied, and this means the customer:

- is willing to accept the bank's actions or the complaint outcome
- expresses no further dissatisfaction
- is 'happy' or 'not unhappy' with the outcome.

There are marked differences is complaint resolution timeframes between banks (**Chart 12**). For comparison purposes, Chart 12 also shows an 'industry average' figure, calculated as the mean average of each individual bank's percentage for each resolution time period.

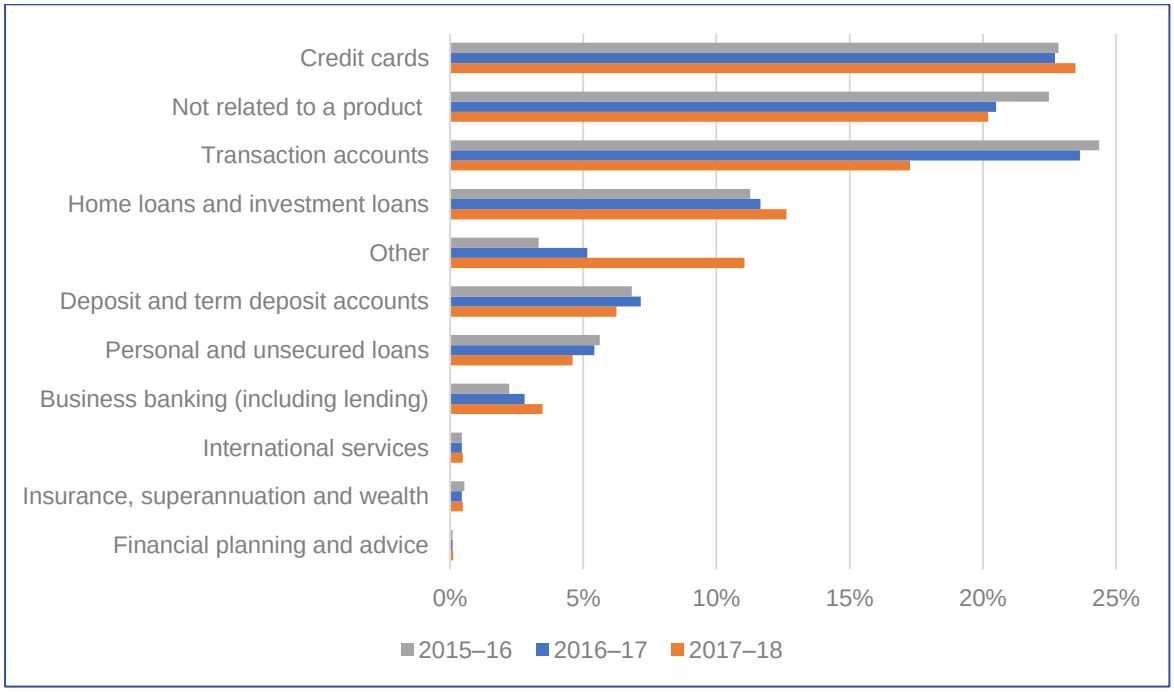
Chart 12. Complaint resolution timeframes, by bank, 2017–18



What customers complain about

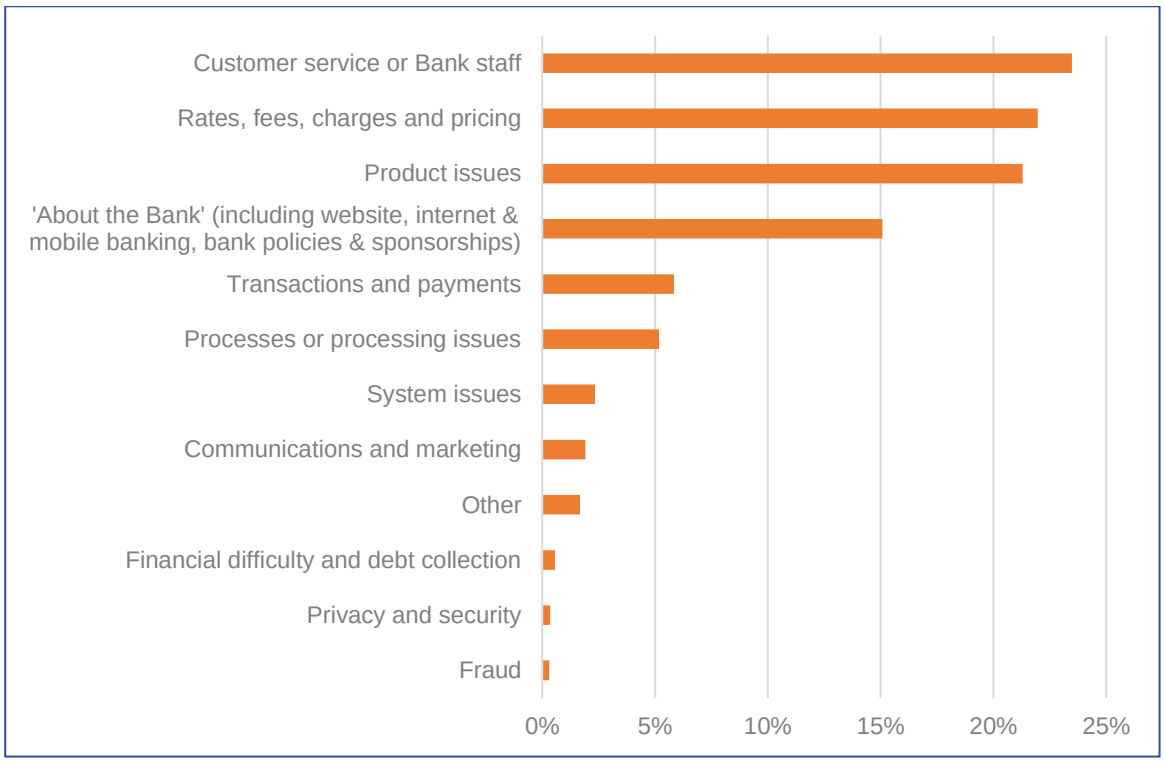
Credit cards (23%), transaction accounts (17%) and complaints not related to a product (20%) continued to be the top areas of concern in 2017–18, consistent with the previous two years (**Chart 13**).

Chart 13. Complaints received, by product, 2015–16 to 2017–18



Complaints were most commonly about customer service or bank staff (23%) and rates, fees, charges or pricing (22%) (**Chart 14**). This year, banks were able to use their own complaint issue categorisation. As a result, the 2017–18 data is more granular, but the categories no longer align for comparison with previous years.

Chart 14. Complaint issues, 2017–18



Breach trends

Banks reported 419 IDR breaches, a 75% increase from 240 in 2016–17 (**Table 27**). Seven of the eight banks reporting IDR breaches saw breaches increase this reporting period. A major bank which accounted for 84% of IDR breaches, reported an increase of 55% between 2016–17 and 2017–18. This bank attributed this increase to a system issue that caused a 48 hour shutdown, disrupting work. IDR was also targeted for risk analysis and assessment, which identified issues. Bank A attributed its 800% breach increase to greater oversight of the complaints data, which identified Code breaches.

Table 27. IDR breaches, by bank, 2017–18

Bank	2016–17	2017–18	Change 2017–18
Big 4	228	353	55%
Big 4	1	30	2,900%
Big 4	3	13	333%
Big 4		10	
Bank A	1	9	800%
Bank B	7	2	-71%
Bank C		1	
Bank D		1	
Total	**240**	**419**	**75%**

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 406 IDR reaches – 97% of the total reported. The rest of this chapter refers only to this subset of 406 breaches.

The nature and impact of the breaches

Most IDR breaches (84%) were due to a customer's dissatisfaction not being recognised and logged as a complaint. A major bank reported some 339 breaches of this type.

The next most common breach type, accounting for 9% of the total, occurred when banks failed to send a customer a final written response. Bank D (**Table 28**) reported one such breach that impacted 560 customers. Complainants may not have been issued with final response letters within the 45-day timeframe. The breach was caused by a combination of a lack of knowledge by key staff and the reporting limitations of a newly introduced complaints management system. A number of system and process controls have since been implemented, and the correct letters were eventually sent to customers.

Three breaches reported by a major bank relate to a failure to respond to financial difficulty assistance request within timeframe. These might be better reported as breaches of the Code's financial difficulty obligations.

There were other breaches where progress letters were not issued within required timeframes or resolution timeframes were not met. The remaining breaches were caused by general customer service issues when handling complaints.

Only one bank identified any financial impact arising from IDR breaches. This major bank reported that the financial impact of two IDR breaches totalled $39,300. This sum was offered in compensation for complaints that were poorly handled by the bank. In one case the compensation was awarded by the bank's Customer Advocate.

Table 28. Impact of IDR breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Big 4	352	372	$ -
Big 4	28	28	$ -
Big 4	12	191	$ -
Bank A	6	6	$ -
Big 4	4	42	$ 39,300
Bank B	2	3	$ -
Bank C	1	1	$ -
Bank D	1	560	$ -
Total	**406**	**1,203**	**$ 39,300**

What caused the breaches and how they were identified

Some 99% of IDR breaches were caused by human error, with more than 90% of these 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 (394 breaches)
- corrected the individual issue (such as recording the complaint) (340)
- held performance management discussions with staff (28)
- apologised to the customer (6)
- enhanced monitoring or controls (5)
- reviewed processes or made improvements (4)
- paid compensation to the customer (3)

Investigations were ongoing for 3 breaches.

How complaints data was used to identify breaches

Complaints play a significant role in the identification of breaches. However, the contribution of complaints to breach identification varies widely between banks (**Table 29**). Two major banks record all complaints, including those resolved within five days, but are notable for the low percentage of breaches identified via complaints. It appears that some banks may not have adequate processes for reviewing complaints to identify breaches, while others may be relying too heavily on complaints for breach identification, without sufficient other monitoring.

Table 29. Percentage of breaches identified due to a complaint or query, by bank, 2017–18

Bank	Total breaches for which details were provided	Breaches identified from customer complaint or query	
Bank A	63	44	70%
Bank B	30	14	47%
Bank C	180	72	40%
Big 4	571	197	35%
Bank D	44	13	30%
Bank E	151	40	26%
Bank F	813	209	26%
Bank G	43	8	19%
Big 4	277	51	18%
Big 4	420	42	10%
Big 4	4,874	17	0.3%
Bank H	9		0%
Bank I	2		0%
Total	**7,477**	**707**	**9%**

Staff training and competency

The Code sets out standards for staff training and competency in clause 9.

Breach trends

Banks reported 84 staff training breaches in 2017–18, a 58% decrease from 202 breaches in 2016–17 (**Table 30**). This decrease reflects reporting changes. A major bank which accounted for more than half of all staff training breaches in 2016–17, this year reported a large drop in breaches. Previously, this bank took a broad approach to reporting breaches of this type, as described by the CCMC in its report on the Code breach reporting inquiry:

> Where staff members are found to have made an error which they would not have made had they dealt with a matter as they were trained to, the bank may report this as a breach of clause 9 […] Other banks only consider matters to be a training and competency breach where training has not been conducted or completed, or where the training is not suitable or effective.[10]

The bank has since reviewed its breach categorisation, and as a result, fewer breaches were identified. Bank C also attributes its reduction in clause 9 breaches to changes in categorisation.

Table 30. Staff training breaches, by bank, 2016–17 to 2017–18

Bank	2016–17	2017–18	Change 2017–18
Bank A	26	32	23%
Big 4	14	19	36%
Big 4	117	17	-85%
Big 4		6	
Bank B	5	5	0%
Big 4	4	5	25%
Bank C	34		-100%
Bank D	2		-100%
Total	**202**	**84**	**-58%**

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 53 staff training breaches – 63% of the total reported. The rest of this chapter refers only to this subset of 53 breaches.

The nature and impact of the breaches

A majority (66%) of staff training and competency breaches occurred where staff performed their role without completing necessary or mandatory training. Most of these breaches were caused by process deficiencies.

[10] CCMC, June 2018, *Own Motion Inquiry: Breach Reporting*.

The remaining 34% of staff training and competency breaches were ‘general’ staff errors, where training was not specifically referenced in the description of the incident. These types of incident made up the majority of breaches reported in 2016–17. Most of these breaches were caused by human error.

Combined, these 53 breaches affected 106 customers and had a total financial impact of $60,882.

How the breaches were identified and corrected

Most staff training breaches (57%) were identified through Line 1 quality assurance monitoring.

Banks undertook one or more of the following corrective actions for each breach:

- provided staff training, coaching or feedback (22 breaches)
- corrected the issue (17)
- enhanced monitoring or controls (7)
- implemented a system fix (4)
- provided the customer with a refund or goodwill payment and/or waived a fee (2)
- held performance management discussions with staff (2)
- reviewed processes and made improvements (2)
- apologised to the customer (2)
- communicated or corresponded with the customer (1).

Corrective actions were still underway for 20 breaches.

Terms and conditions

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

Breach trends

Banks reported 200 terms and conditions breaches in 2017–18. This is a substantial increase of 139 (228%) from 2016–17 (**Table 31**).

Table 31. Terms and conditions breaches, by bank, 2016–17 to 2017–18

Bank	2016–17	2017–18	Change 2017–18
Big 4	4	103	2,475%
Big 4	19	56	195%
Big 4	6	14	133%
Bank A	4	11	175%
Bank B	12	2	-83%
Bank C	7	4	-43%
Big 4	5	2	-60%
Bank D	4	2	-50%
Bank E		5	
Bank F		1	
Total	**61**	**200**	**228%**

The rise in terms and conditions breaches was driven primarily by two major banks. These banks saw breaches increase by 99 (2,475%) and 37 (195%) respectively. Together, these banks accounted for 80% of terms and conditions breaches in 2017–18. Both banks attributed the increases to monitoring improvements. The bank that reported 103 breaches explained that its retail branch risk team expanded its assurance resources and capability and performed more branch monitoring and assurance reviews. As part of this, account opening procedures were monitored and on some occasions, terms and conditions were not provided. The other bank also stated that breaches increased because it improved monitoring and identification of Code breaches.

Conversely, one bank, Bank A, attributed its breach increase to terms and conditions not being sufficiently clear for customers. Bank A was in the process of taking steps to address this.

Four banks did not disclose any terms and condition breaches.

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 170 terms and conditions breaches – 85% of the total reported. The rest of this chapter refers only to this subset of 170 breaches.

The nature of the breaches

Most breaches (78%) involved terms and conditions that were issued incorrectly or not at all (**Table 32**). Positively, there was a reduction in the percentage of breaches about a failure to comply with terms and conditions – down from 25% in 2016–17 to 6% this year. The CCMC noted previously that such breaches should instead be reported under clause 3 (key commitments), so this trend may indicate reporting improvements.

Table 32. Types of terms and conditions breaches, 2017–18

Type of Incident	Breaches	Percentage of breaches
Terms and conditions not issued or issued incorrectly	132	78%
Terms and conditions contained incorrect information or missing information	25	15%
Terms and conditions not complied with	10	6%
Information in terms and conditions was not clear	2	1%
Statements displaying incorrect or inaccurate information	1	1%
Total	**170**	

What caused the breaches

Cited in 140 breaches (82%), human error was the most common cause of terms and conditions breaches, although there was often another contributing cause. A control, training or resourcing failure was cited as a cause in 110 breaches (65%).

How the breaches were identified

Most terms and conditions breaches (102 or 60%) were at least partly identified through internal review or audit. Reporting by a staff member accounted for 27 breaches (16%) while quality assurance and monitoring identified 22 breaches (13%).

The impact of the breaches

In 2017–18, terms and conditions breaches affected 128,446 customers, with a total financial impact of $603,629 (**Table 33**).

Table 33. Impact of terms and conditions breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact	
Big 4	101	26,104	$	-
Big 4	36	46,297	$	110,999
Big 4	12	11,065	$	500
Bank A	6	6,519	$	17,695
Bank B	5	37,138	$	473,375
Bank C	4	1,282	$	1,000
Bank D	2	37	$	-
Bank E	2	1	$	5
Big 4	1	1	$	55

Bank	Breaches	Customers impacted	Financial impact
Bank F	1	2	$ -
Total	**170**	**128,446**	**$ 603,629**

A breach by Bank B had a financial impact of $403,000. The breach occurred due to a long-standing error, calculating the difference between promotional and non-promotional rates. With the error occurring since at least 2014, some 36,000 customers have been affected. Bank B has implemented a system fix and is refunding customers.

How the breaches were corrected

Banks' action to correct terms and conditions breaches were focused on preventing recurrence rather than addressing impacts on individual customers (**Table 34**). However, it should be noted that addressing the individual impacts of a single breach could entail remediating many thousands of customers, as in the Bank B example above.

Table 34. Type of corrective action for terms and conditions breaches, by bank, 2017–18

Bank	Preventing recurrence	Both	Remediating customer	Investigations ongoing
Big 4	100 (99%)	1 (1%)		
Big 4	23 (64%)	8 (22%)	3 (8%)	2 (6%)
Big 4	1 (8%)	3 (25%)	4 (33%)	4 (33%)
Bank A	2 (33%)	1 (17%)	3 (50%)	
Bank B		4 (80%)		1 (20%)
Bank C	1 (25%)	1 (25%)	1 (25%)	1 (25%)
Bank D	1 (50%)		1 (50%)	
Bank E		1 (50%)		1 (50%)
Big 4		1 (100%)		
Bank F			1 (100%)	
Total	**128 (75%)**	**20 (12%)**	**13 (8%)**	**9 (5%)**

To prevent recurrence, banks most often:

- provided staff training, coaching or feedback (119)
- implemented a system fix (23)
- process review/ improvements (9)
- enhanced monitoring and controls (6)

To address customer impacts, banks:

- refunded, reimbursed or otherwise compensated customers (19)
- communicated or corresponded with the customer (15)
- corrected an individual issue (5)
- apologised to the customer (3).

For 9 breaches, banks indicated no action had been taken as investigations were ongoing or no action was needed.

Compliance with laws

With clause 4 of the Code, banks commit to comply with all relevant laws. The CCMC's compliance monitoring functions and powers, however, only extend to clause 4 where a breach of this clause is also a breach of another provision of the Code.

The CCMC has 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 accommodates this approach and consequently some banks – but not all – do report compliance with laws breaches.

Breach trends

Banks reported 594 compliance with laws breaches, a 6% decrease from 632 in 2016–17.

Bank A (**Table 35**) accounted for the most compliance with laws breaches in 2016–17. Following an increase to 403 breaches, Bank A also made up 68% of total compliance with laws breaches in 2017–18.

Table 35. Compliance with laws breaches, by bank, 2016–17 and 2017–18

Bank	2016–17	2017–18	Change 2017–18
Bank A	342	403	18%
Bank B	54	86	59%
Big 4	78	36	-54%
Bank C	19	21	11%
Bank D	23	10	-57%
Bank E	15	9	-40%
Bank F	4	8	100%
Bank G	19	8	-58%
Bank H	24	7	-71%
Big 4	33	6	-82%
Big 4	20		-100%
Bank I	1		-100%
Total	**632**	**594**	**-6%**

Four banks reported no compliance with laws breaches. Due to the broad nature of clause 4, breaches are likely. Therefore, where larger banks report no clause 4 breaches, the CCMC expects that this reflects a decision not to report, rather than an absence of breaches.

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 538 compliance with laws breaches – 91% of the total reported. The rest of this chapter refers only to this subset of 538 breaches.

The nature of the breaches

Compliance with laws breaches were most commonly the result of:

- failure to verify a customer's identity (164 breaches, 30%)

- advertised information being incorrect (124 breaches, 23%)
- operational errors (87 breaches,16%)
- not providing financial advice in a customer's best interest (84 breaches, 16%).

Clause 4 requires banks to comply with all relevant laws relating to banking services, without specifying these laws. Banks identified the specific law breached for only 56 breaches. The CCMC will request banks stipulate the relevant law when reporting compliance with laws breaches in future.

Table 36 provides details of the legislation cited and most common types of issues related to that legislation, and the percentage of breaches the issue accounted for.

Table 36. Specified legislation and the most common type of issue for each, 2017–18

Legislation	Breaches	Percentage of breaches caused by issue
Corporations Act 2001 (Cth)	**23**	
Failure to provide financial advice in the customer best interest		92%
Foreign Account Tax Compliance Act (US)	**9**	
Monitoring failures		56%
AUSTRAC administered legislation	**8**	
Failure to report matters to the relevant statutory authority		50%
E-payments Code	**8**	
Operational errors		38%
National Consumer Credit Protection Act 2009 (Cth)	**4**	
Bank did not lend responsibly		50%
Banking Act 1959 (Cth)	**2**	
Monitoring failures		50%

How the breaches were identified

Most compliance with laws breaches (352 or 65%) were identified partly through quality assurance and call monitoring. Staff members identified 159 breaches (30%), while 107 breaches (20%) were identified through internal audit or internal reviews. Customer complaints or queries contributed to identification of 35 breaches (7%).

The impact of the breaches

Compliance with laws breaches had a substantial impact, likely due to the broad nature of clause 4. Some 733,148 customers were impacted by compliance with laws breaches in 2017–18, while the total financial impact was more than $9.4 million (**Table 37**).

Combined, breaches by Bank F impacted the largest number of customers – 416,002, or 57% of the total. A single breach affected 416,00 customers, between October 2016 and October 2017, when customers did not receive email notification when their statements were made available in internet banking.

A major bank accounted for the largest share of the financial impact – $5,275,291 or 56% of the total. Some $3,240,000 of this impact resulted from one breach concerning a subsidiary's provision of ongoing advice services. Another $1,750,000 was attributable to incorrect terms and conditions concerning a product's minimum deposit information. The terms and conditions have been updated and a remediation program has begun.

Bank D was responsible for $3,180,463 in financial impact – around a third of the total. One breach had a $3 million impact when transactions that had already been processed in March 2017 were wrongly processed for a second time in August 2017. Bank D responded by reversing the payments and instituting further checks on transactions.

Table 37. Impact of compliance with laws breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Bank A	388	187,653	$ 498,936
Bank B	86	5,992	$ 318,172
Big 4	36	38,897	$ 5,275,291
Bank C	8	740	$ 158,000
Bank D	8	80,851	$ 3,180,463
Big 4	5	3,009	$ 3,250
Bank E	4	4	$ -
Bank F	2	416,002	$ -
Bank G	1	0	$ -
Total	**538**	**733,148**	**$ 9,434,113**

How the breaches were corrected

The main actions taken by banks to remedy compliance with laws breaches were:

- providing staff training, coaching or feedback (316)
- correcting an individual issue (253)
- enhancing monitoring and controls (131)
- reviewing process and/or made improvements (79)
- refunding, reimbursing or otherwise compensating customers (38)
- communicating or corresponding with the customer (20)
- correcting or updating details (20)
- referring the matter to a regulator (7).

Privacy and confidentiality

The Code's privacy and confidentiality requirements are set out in clause 24.

Breach trends

Banks reported 4,464 privacy and confidentiality breaches in 2017–18, a 63% increase from 2,743 in 2016–17. As with previous years, one outlier major bank reported the majority of privacy and confidentiality breaches (2,767 or 62% of the total) and saw such breaches increase by 62% to 2017–18. However, the major bank alone does not account alone for the upwards trend: all but four banks reported an increase in privacy and confidentiality breaches from 2016–17 to 2017–18.

Table 38. Privacy and confidentiality breaches, by bank, 2016–17 to 2017–18

Bank	2016–17	2017–18	Change 2017–18
Big 4	1,706	2,767	62%
Big 4	101	428	324%
Big 4	148	264	78%
Big 4	178	240	35%
Bank A	229	233	2%
Bank B	72	229	218%
Bank C	93	131	41%
Bank D	146	96	-34%
Bank E	10	23	130%
Bank F	12	20	67%
Bank G	29	18	-38%
Bank H	18	15	-17%
Bank I	1		-100%
Total	**2,743**	**4,464**	**63%**

Seven banks provided a specific reason for the rise in privacy and confidentiality breaches. The outlier bank and five others (two major banks, Bank B, Bank C, and Bank E) stated the rise was due to improved monitoring of privacy and confidentiality breaches, such as through new monitoring initiatives and staff awareness. The remaining major bank stated that the increase resulted from reclassification.

Two banks reported decreases in privacy and confidentiality breaches. Bank D said that the decrease was achieved with greater staff training, while Bank G attributed the decrease to a change in how it classifies Code breaches.

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 2,876 privacy and confidentiality breaches – 64% of the total reported. The rest of this chapter refers only to this subset of 2,876 breaches.

The nature of the breaches

Information provided or disclosed to an incorrect party and identification errors were the main breach types, accounting for 30% and 29% of breaches respectively. Tax File Number (TFN) issues also contributed 12% of breaches.

Table 39. Types of privacy and confidentiality breaches, 2017–18

Issue type	Breaches	Percentage of breaches
Information provided or disclosed to incorrect party	874	30%
Identification errors	833	29%
TFN issues	345	12%
Privacy policy scripting not read or not disclosed	181	6%
Documentation or contracts sent electronically without being encrypted/secured	177	6%
Credit bureau or reference check issues	142	5%
Document or information security issues	39	1%
Unauthorised access of account	28	1%
Other	257	9%
Total	**2,876**	

What caused the breaches

An overwhelming majority of privacy and confidentiality breaches (2,840 or 99%) included human error as a cause. A system error, failure or issue accounted in part for 43 breaches, while misconduct and fraud accounted in part for 22 breaches.

How the breaches were identified

A significant majority of 2,245 (78%) of privacy and confidentiality breaches were identified through quality assurance and call monitoring. Customers and staff members also contributed, with customer complaints and queries and staff member reporting contributing to the identification of 569 (20%) and 371 (13%) breaches respectively.

The impact of the breaches

Some 465,166 customers were impacted by privacy and confidentiality breaches in 2017–18, however, the financial impact of these breaches was comparatively low at $678,656 (**Table 40**).

One set of breaches by a major bank accounted for 420,056 of the customers affected – 90% of the total. The breaches occurred when customer and personal information was mistakenly published on a bank knowledge sharing system or intranet. Once identified, the offending files were taken down, and the bank conducted an investigation that included staff feedback and testing of the relevant controls.

Three-quarters of the financial impact of privacy and confidentiality breaches ($508,066) relates to one breach by Bank F. A personal term deposit was manually linked to the incorrect bank account, causing one customer's closing balance to be deposited into another customer's account. When the bank identified the breach, it placed a hold on the relevant account and recovered the funds. Bank F also updated its manual account operating procedure.

Table 40. Impact of privacy and confidentiality breaches, by bank, 2017–18

Bank	Breaches	Customers impacted	Financial impact
Big 4	2,100	16,653	$ 23,000
Bank A	211	1,712	$ 11,893
Big 4	209	1,246	$ 5,074
Big 4	110	18,280	$ 83,127
Bank B	87	2,148	$ -
Big 4	76	420,086	$ 44,977
Bank C	20	263	$ -
Bank D	18	41	$ 1,221
Bank E	17	2,271	$ -
Bank F	14	384	$ 508,066
Bank G	11	2,076	$ 1,297
Bank H	3	6	$ -
Total	**2,876**	**465,166**	**$ 678,656**

How the breaches were corrected

Banks reported a range of steps to correct the breaches (**Table 41**). Most commonly, this included steps to prevent recurrence of the breach.

Table 41. Types of corrective action for privacy and confidentiality breaches, by bank, 2017–18

Bank	Preventing recurrence	Both	Remediating customer	Investigations ongoing
Big 4	1,341 (64%)	741 (35%)	13 (1%)	5 (0%)
Big 4	68 (89%)	5 (7%)	2 (3%)	1 (1%)
Bank A	38 (18%)	127 (60%)	43 (20%)	3 (1%)
Big 4	18 (9%)	188 (90%)	3 (1%)	
Big 4	13 (12%)	82 (75%)	13 (12%)	2 (2%)
Bank B	12 (14%)		75 (86%)	
Bank C	9 (45%)	3 (15%)	1 (5%)	7 (35%)
Bank D	2 (14%)	12 (86%)		
Bank E	2 (18%)	9 (82%)		
Bank F	1 (6%)	16 (89%)	1 (6%)	
Bank G	1 (6%)	9 (53%)	6 (35%)	1 (6%)
Bank H		3 (100%)		
Total	**1,505 (52%)**	**1,195 (42%)**	**157 (5%)**	**19 (1%)**

To prevent recurrence, banks most commonly:

- provided staff training, coaching or feedback (2,643)
- held performance management discussions with staff (1,239)
- reviewed or improved processes (82)
- enhanced monitoring and controls (35)
- implemented a system fix (5).

To address customer impacts, banks:

- corrected an individual issue (794)
- apologised to the customer (554)
- corrected or updated details (204)
- requested that information be destroyed, deleted or returned (185)
- communicated or corresponded with the customer (100)
- refunded, reimbursed or otherwise compensated customers (13).

For 19 breaches, bank responses indicated corrective actions were still being considered.

Direct debits

Under clause 21 of the Code, banks must take and promptly process a customer's instruction to cancel a direct debit request. Banks are not permitted to direct or suggest that the customer should first ask the relevant merchant or service provider to cancel the direct debit, although banks can suggest that the customer also contact the merchant or service provider. Banks must also take and promptly process any complaint that a direct debit was unauthorised or otherwise irregular.

Banks' compliance with the direct debit obligations is an area of ongoing focus for the CCMC.

Breach trends

Banks reported 172 direct debits breaches, an 85% increase from 93 in 2016–17 (**Table 42**). The increase can be largely attributed to one major bank, whose breaches increased 229% from 38 to 125 between 2016–17 and 2017–18. This bank attributes the increase to breach identification improvements. In the past year, the bank established a centralised first line risk team that is accountable for monitoring and providing quality assurance concerning events and breaches in the bank's incident and breach register. Face-to-face training built staff skill in identifying and correctly reporting breaches. A monthly quality assurance process tracks the team's quality, efficiency and adherence to set processes.

Table 42. Direct debit breaches, by bank, 2016–17 to 2017–18

Bank	2016–17	2017–18	Change 2017–18
Big 4	38	125	229%
Big 4	18	22	22%
Bank A	14	16	14%
Bank B		3	
Bank C	1	2	100%
Bank D	1	2	100%
Big 4	19	2	-89%
Big 4	1		-100%
Bank E	1		-100%
Total	**93**	**172**	**85%**

Following the CCMC's reporting instructions (see p. 5), banks provided further information about the nature, cause, impact and correction of 50 direct debits breaches – 29% of the total reported. The rest of this chapter refers only to this subset of 50 breaches.

The nature, cause and impact of the breaches

Most direct debit breaches (80%) concerned a bank's failure to cancel a direct debit at a customer's request. In four cases the bank provided the customer with incorrect direct debit cancellation information. Six direct debit requests may not have been a breach the Code. In these cases, there were direct debit processing issues or a request to cancel recurring card payment was processed incorrectly. The Code obligations do not cover recurring card payments.

Two direct debit breaches were caused by deficient training or processes. The remaining 96% were caused by human error.

The 50 direct debits breaches affected 52 customers and had a total financial impact of $12,235. The CCMC would expect to see a one for one ratio between breaches and number of customers impacted, unless the issue was considered systemic.

How the breaches were identified and corrected

Most direct debit breaches (82%) continue to be identified as a result of customer complaints (this accounted for 77% of breaches in 2016–17). However, we note from one bank's response above regarding the increase in breaches, that many of the total number (172) may have been identified through quality assurance monitoring of frontline staff.

Generally, banks are thorough when correcting direct debits breaches, usually taking multiple actions to prevent recurrence and address customer impacts. For each breach, banks took one or more of the following actions:

- provided staff with further training, coaching or feedback (47)
- corrected the issue, typically by cancelling the direct debit (35)
- provided the customer with a refund or goodwill payment (27)
- apologised to the customer (27)
- enhanced monitoring or controls (3).

CCMC is conducting ongoing monitoring of the Code's direct debit obligations and will issue an update report in early 2019.

Other Code obligations

Banks reported 327 breaches of other Code obligations (**Table 43**).

Table 43. Breaches of other obligations, 2016–17 to 2017–18

Code obligation	2016–17	2017–18	Change 2017–18
Pre-contractual and new account information	10	124	1,140%
Availability of copies of the Code	2	35	1,650%
Electronic communications	76	30	–61%
Operation of accounts	13	23	77%
Statement of account	22	21	–5%
Chargebacks	28	17	–39%
Closure of accounts in credit	25	15	–40%
Cost of credit	13	12	–8%
Changes to terms and conditions	12	7	–42%
Information relating to foreign exchange services	12	6	–50%
Joint accounts and subsidiary cards	4	6	50%
Availability of information about dispute resolution process	2	6	200%
Copies of documents	20	5	–75%
Account suitability	4	5	25%
Bank cheques and inter-bank transfers	3	5	67%
Joint debtors	5	3	–40%
Payment and instruments	14	2	–86%
Branch closure protocol	2	2	0%
Customers with special needs	8	1	–88%
Account combination	2	1	–50%
External Dispute Resolution	0	1	–
Promotion of the Code	13	0	–100%
Retention of your rights	0	0	–
Review of the Code	0	0	–
Customers in remote Indigenous communities	0	0	–
Monitoring and sanctions	0	0	–
Family law proceedings	0	0	–
Total	**290**	**327**	**13%**

A major bank reported 92% of the precontractual and new account information breaches. Most (100) of these breaches occurred where fees incurred during the loan process were not detailed. The bank attributed the increase to an improved, more granular, approach to identifying Code breaches.

Another major bank reported 97% of the breaches concerning availability of copies of the Code. In these cases, copies of the Code were not on display in branches. Understandably the bank is unable to determine any customer or financial impact.

Banks provided details of 271 of these 327 breaches, following the CCMC's reporting instructions (see p. 5). Collectively the breaches impacted 566,518 customers and had a financial impact of $598,420.

Examples of some of the breaches with a higher customer impact are provided in **Table 44**.

Table 44. High-impact breaches of other Code obligations

Code clause	Breaches	Description of incident/ corrective actions	Customers impacted	Financial impact
Customers with special needs	1	FOS systemic issue. Failure to have adequate guidelines or training in relation to the identification of possible financial abuse of elders. Roll out of revised policies and procedures.	2	$ 139,000
Payment and instruments	1	Loan was approved outside of the lenders authority. Income assessment was incorrect due to outstanding tax and statutory charges declaration. Lender responsible for error no longer employed therefore no additional training could be undertaken.	2	$ 215,715
Changes to terms and conditions	1	Failure to send a 'Notice of Change' to selected credit card customers informing them of the changes associated with a credit card relaunch. Notice of change was re-issued with new effective date of change. Bank will honour the existing reward terms and conditions.	17,000	$ 17,482
Statement of account	6	Failure to provide statements as required. Project established to fully investigate and remediate all causes. Reported to ASIC as a breach of obligations under the *Corporations Act 2001 (Cth)*.	478,000	$ -
Statement of account	1	Statements not issued – system issue. Reversal of fees and interest incurred as a result of the issue. System fix.	15,435	$ 147,207
Branch closure protocol	1	Incorrect information about branch closure provided to customers. New controls and procedures introduced	7,800	$ -

Code clause	Breaches	Description of incident/ corrective actions	Customers impacted	Financial impact
Electronic communications	2	Secure message has not been sent to customer to advise them that their statement is available and to ask them to update contact details when a 'hard bounce back' is received from a notification of online statement availability. Incident still in progress, awaiting a permanent system fix in Internet Banking. A secure message is sent to customers when a bounce back is received.	17,633	$ -
Electronic communications	1	Customer contracts issued via email without written consent. Process implemented to gain customer consent for electronic communication. Staff training.	25,000	$ -