BANKING CODE COMPLIANCE MONITORING COMMITTEE

REPORT:

Own Motion Inquiry: Breach Reporting

JUNE 2018

Contents

1 Executive summary

In order to monitor compliance with the Code of Banking Practice (the Code), the Banking Code Compliance Monitoring Committee (CCMC) relies on breach data reported by banks. In recent years the CCMC has identified inconsistencies in how banks record and report Code breaches.

To better understand banks' data and to improve its data collection strategy, the CCMC conducted this Own Motion Inquiry (the inquiry) into banks' reporting of Code breaches.

For this inquiry, the CCMC asked banks to provide further information about breaches that were previously reported in the 2016–17 Annual Compliance Statement (ACS), the CCMC's core data collection tool.

This report outlines the CCMC's key findings and the most important of these findings are highlighted in this summary.

Overall the CCMC was satisfied with banks' responses to the inquiry. The detailed nature of the information provided has enabled the CCMC to identify specific areas where it can outline its expectations to improve the accuracy, completeness and consistency of its data collection. Where there are specific areas of concern with a bank, the CCMC will work directly with that bank to address these issues.

More broadly, the CCMC wants to continue to work with banks to improve its data collection and reporting so that the self-regulatory compliance framework operates more effectively.

1.1 Breach numbers

By asking banks to conduct an in-depth review of their breach data, some banks reclassified some breach incidents previously reported in the 2016–17 ACS. This meant that the numbers of reported beaches for most of the Code obligations covered in this report are lower than the figures in the CCMC's 2016–17 Annual Report. However, one bank's large increase in reported debt collection breaches meant that overall, the number of reported breaches was higher (see section 3.1 of the Report).

The CCMC expects banks to be diligent at all times in providing accurate and complete data in response to requests for information.

1.2 Causes of Code breaches

Across all areas, human error was consistently reported by banks to be the primary contributor to Code breaches.

While human error cannot always be avoided, the CCMC expects banks to use breach data to identify patterns and develop systems and system controls that prevent repeated errors.

Despite the dominant role of human error as a cause of breaches, banks only rarely identified associated deficiencies in staff training. For example, while human error was reported by banks as the cause of 99% of provision of credit breaches, banks concluded that training had been inadequate in just a tiny fraction of cases (4 out of 4,135 breaches) (see section 4.2.3).

The CCMC expects banks to use information about breaches caused by human error to review the effectiveness of staff training.

1.3 Identification of breaches

Banks typically identify Code breaches through one of a range of proactive monitoring activities. Almost two-thirds (64%) of all Code breaches were identified through the monitoring of telephone calls, while 'Line 1'[1] quality assurance (QA) activities also identified many breaches (see section 3.3). Banks also become aware of breaches when customers notify the bank of a problem or lodge an IDR or external dispute resolution complaint.

Different breach identification methods are used by the banks depending on the Code obligation being monitored. While most breaches are identified through banks' proactive monitoring activities, direct debits is an exception. Here, most reported breaches are identified only as a result of customer complaints, which may suggest that many breaches are not being identified or corrected. The CCMC has previously recommended banks take a more proactive approach to the monitoring of the direct debits Code obligations (see section 7.2.2).

1.4 Customer impact

Breach numbers alone do not give a full sense of the magnitude of an issue. The 9,872 breaches reported for 2016–17 affected some 152,830 customers, demonstrating that while some breaches affect only a single customer, the impact is often much wider. Different Code obligations are associated with different levels of customer impact. For instance, breaches of the Code's IDR provisions tend to have a contained impact, whereas terms and conditions breaches can affect many thousands of customers.

In some cases, it appears that banks have not fully investigated and tracked the impact of Code breaches. For example, one bank reported almost 3,000 provision of credit breaches resulting from two types of incidents, but stated that these breaches were unlikely to have an effect on customers (see section 4.2.1). The CCMC expects banks to fully investigate how each breach has impacted customers.

The CCMC also requested data on the financial impact of breaches for customers. However, this data was of limited value and the CCMC will explore this issue with banks to develop a more consistent reporting approach for financial impact information.

[1] 'Line 1' is a reference to the three lines of defence model for risk and compliance management.

1.5 Corrective actions

For around one-quarter of the Code breaches identified, banks did not report any associated corrective action (see section 3.4).

Moreover, where corrective actions were reported, banks tended to focus heavily on preventing re-occurrence (for example, with staff training), without also taking action to address the impact of the breach on customers. For example, when correcting provision of credit breaches, banks generally appeared not to have considered or addressed how inappropriate or irresponsible lending affected the customer.

Corrective actions may not have occurred, or they may not have been recorded in a bank's incident management system or reported to the CCMC. The CCMC expects banks to remediate customers appropriately and to record and report all corrective actions.

1.6 Monitoring

The CCMC also asked banks about their activities for monitoring compliance with the Code. Whilst banks' responses broadly suggest they have adequate monitoring programs, the CCMC did identify some areas of concern.

Across the industry, comprehensive call monitoring and quality assurance programmes are used to assess compliance and the quality of staff members' interactions with customers. The inquiry identified many good monitoring practices, with particularly strong monitoring frameworks for the provision of credit at most banks (see section 4.3).

The CCMC's primary concern with regard to monitoring is that banks provided minimal or no information about how they monitor and test systems. For instance, banks had little to say about how they test the dialling and case management systems used in debt collection, the systems used in decision making on the provision of credit, or IDR case management systems. Wherever banks rely on systems to fulfil their obligations to customers, the CCMC expects them to test these systems regularly and comprehensively.

1.7 Next steps

The CCMC will provide feedback to each bank to ensure that its overall findings and bank specific matters are considered when the bank completes its 2017–18 Annual Compliance Statement.

The CCMC also intends to:

- provide banks with further guidance on its expectations for Code monitoring, and
- use the data gathered through the inquiry to inform its future monitoring activities.

The CCMC will report outcomes from this work in its Annual Reports.

2 Introduction

The CCMC relies on information reported to it by Code-subscribing banks (banks) to monitor compliance with the Code. However, in recent years, the CCMC has identified significant inconsistencies in the way that banks identify and report on Code breaches in the Annual Compliance Statement (ACS), the CCMC's core data collection tool.[2]

To better understand the data reported by banks through the 2016–17 ACS and to enhance its future data collection strategy, the CCMC conducted this Own Motion Inquiry (the inquiry) into banks' reporting of Code breaches. This inquiry contributes to the CCMC's broader aim of delivering a comprehensive and meaningful monitoring program. With a better understanding of how banks report, the CCMC can produce more robust analyses of banks' compliance, translating the data into insights that inform the community and guide improvement to banks practices.

2.1 Purpose of the Inquiry

The CCMC established this inquiry into banks' reporting of Code breaches to benchmark and report to industry and the wider community on banks' monitoring practices, and compliance with the Code.

The inquiry also assists the CCMC to:

- deliver robust analysis of banks' compliance with their Code obligations, as recommended in the independent reviews of the Code of Banking Practice and CCMC
- improve the quality, consistency and reliability of data reported to the CCMC, and
- develop a comprehensive monitoring program for 2017–18 and beyond by establishing priorities for monitoring and a more robust strategy for data collection.

2.2 Inquiry approach

This inquiry, which relates to the banks' 2016–17 ACS, took place between January and June 2018 in three stages: data gathering through a questionnaire completed by all 13 banks subscribing to the Code that year (see Appendix 1), verification and analysis of data, and consultation and reporting.

The CCMC asked banks for information about the top 10[3] Code breach categories by number of breaches reported in the 2016–17 Annual Compliance Statement (ACS). Requested information included:

- a description of what occurred for each breach

[2] The CCMC's monitoring powers are set out in clause 5.1 of its Mandate. In addition, clause 36(f) of the Code and clause 5.2 of the Mandate require banks to lodge an Annual Compliance Statement with the CCMC, reporting on its compliance with the Code during the previous 12 months.
[3] The top 10 excludes key commitments (clause 3) and compliance with laws (4). Code clause 36(b)iii states that the CCMC's compliance monitoring functions and powers do not extend to clauses 3 and 4 of the Code unless a breach of clause 3 or 4 is also a breach of another provision of the Code.

- what caused the breaches
- how banks identified the breach
- what corrective or remedial actions were taken
- the impact of the breach (the number of customers affected and the financial impact on those customers), and
- what monitoring they undertake to ensure compliance with some of the Code obligations and identify any non-compliance.

To contextualise breach numbers, the CCMC also asked for data on the number of related interactions between banks and their customers.

3 Overall compliance and reporting

As well as investigating different areas of Code obligation individually, for this inquiry the CCMC examined overall Code compliance and how it is reported. The CCMC considered overall breach numbers, the causes of breaches, their impacts, and how banks identify and correct breaches.

3.1 Breach numbers

As a result of the inquiry, banks revised upwards the number of breaches previously reported. In the ACS, banks reported a total of 9,083 breaches. For this inquiry, eight banks reassessed and amended their breach data, leading to an overall increase of 789 breaches. This was mainly due to an increase in the number of debt collection breaches reported by one bank.

The CCMC understands that reporting errors can occur, particularly where subjective judgements are required. However, the CCMC expects banks to be diligent about providing accurate and complete data because later corrections are not always possible.

Table 1: Breach reporting differences, ACS and Inquiry

Code obligation	ACS	Inquiry	Variance
Provision of credit (clause 27)	4,200	4,178	-22
Privacy and confidentiality (24)	2,779	2,743	-36
Debt collection (32)	1,119	2,061	+942
Internal dispute resolution (37)	285	240	-45
Staff training and competency (9)	213	202	-11
Financial difficulty (28)	207	183	-24
Direct debits (21)	95	93	-2
Electronic communications (35)	76	76	
Terms and conditions (12)	65	60	-5
Guarantees (31)	44	36	-8
Total	**9,083**	**9,872**	**+789**

3.2 Cause of Code breaches

Banks reported that most Code breaches resulted from multiple contributing factors (Table 2). Human error was involved in almost all (98%) of the Code breaches and 75% involved a process not being followed or a process deficiency. Training and monitoring issues also contributed.

Table 2: Cause of breaches

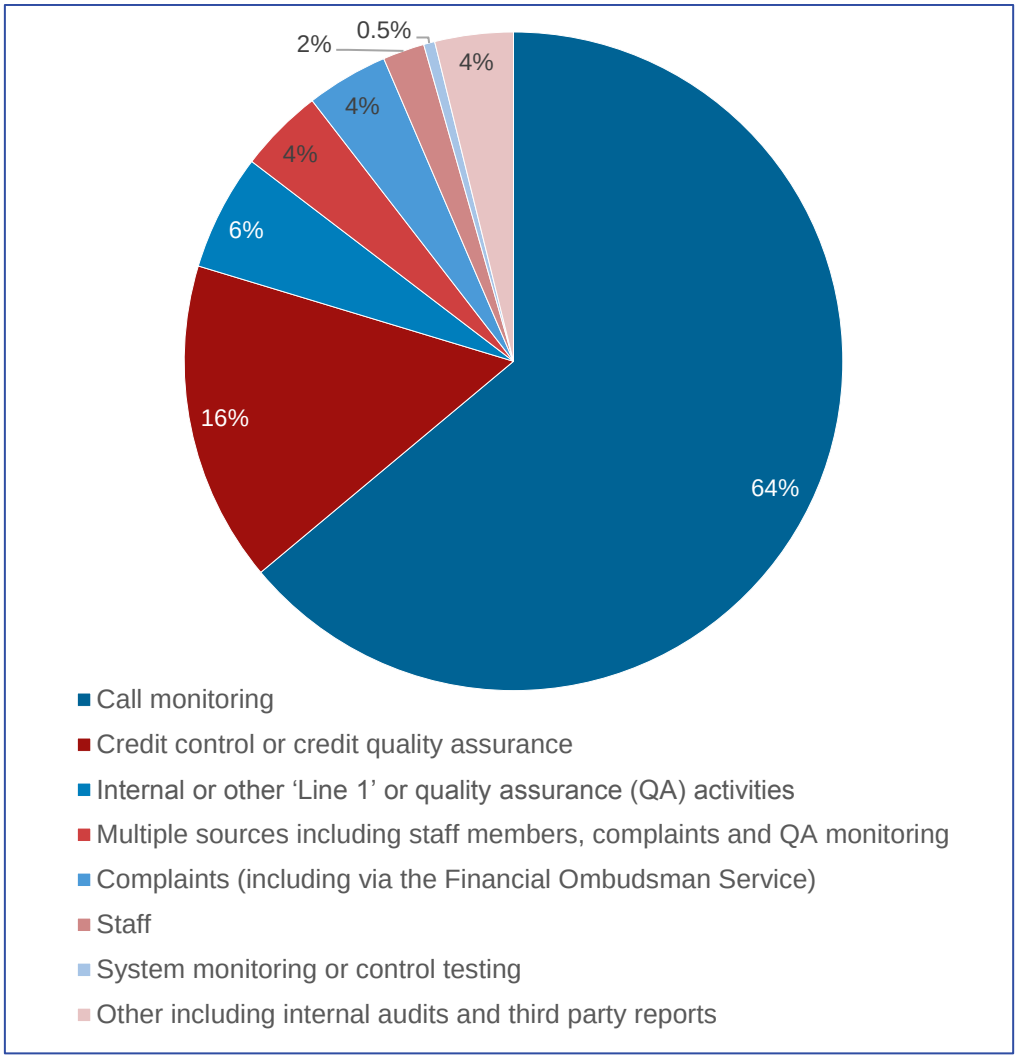
Cause	No. of breaches
Human error	9,667
Process not being followed or process deficiency	7,407
System error	147
Fraud or staff misconduct	22

The CCMC expects banks to use this kind of breach data to look for process gaps and implement effective systems and controls that prevent human error. The CCMC also expects banks to regularly review the effectiveness of staff training.

3.3 Identification of breaches

Banks identified almost two-thirds (64%) of Code breaches through call monitoring. The methods of identification are displayed in **Chart 1**.

Chart 1: Identification of breaches



3.4 Corrective actions

Banks were more likely to report corrective actions taken to prevent an incident from recurring (such as staff training or coaching) than action taken to deal with the impact of breach on a particular customer. For 5,168 breaches, banks reported taking multiple actions to correct the breach. Most commonly, these corrective actions included:

- providing staff training or coaching (4,775 breaches)
- enhancing monitoring or controls (1,005)
- correcting the issue (672)
- apologising to the customer (379)
- providing the customer with a refund or goodwill payment (215)
- implementing a system fix (137).

Where banks listed a single corrective action, the most common of these were:

- providing staff training, coaching or feedback (1,472 breaches)
- logging, managing or resolving complaint (228)
- communicating or corresponding with the customer (92)
- providing the customer with a refund or goodwill payment (73)
- correcting the issue (73)
- requesting that information be destroyed, deleted or returned (61)
- implementing a system fix (44)
- correcting details (25).

For around one-quarter of total breaches, banks did not report any corrective actions. Concerningly, five banks reported a total of 2,567 breaches without corresponding corrective action – either because it was not recorded in the bank's incident management system, or because this information was not reported to the CCMC.

The CCMC expects banks to remediate customers appropriately and to record these actions in their internal systems alongside any action taken to prevent breaches from reoccurring. Both types of action should be reported to the CCMC upon request.

3.5 Customer impact

Data on the number of customers affected by each breach reveals more about the impact of breaches than breach numbers alone. The CCMC noted in its 2016–17 Annual Report that one bank reports a disproportionate number of breaches (Bank A in Table 3). Despite the large number of breaches, however, the number of customers affected was in line with several other banks. At the same time, Bank D and Bank G reported a relatively small number of breaches with very widespread customer impact.

Table 3: Breach impact by bank

Bank	No. of breaches	No. of customers impacted
Bank A	8,032	8,733
Bank B	401	7,534
Bank C	292	6,118
Bank D	265	82,837
Bank E	200	362
Bank F	191	305
Bank G	189	26,041
Bank H	137	134
Bank I	92	9,011
Bank J	38	644
Bank K	24	3,858
Bank L	10	7,245
Bank M	1	8
Total	**9,872**	**152,830**

Similarly, this data shows that breaches of some Code obligations tend to affect more customers. A low number of breaches does not necessarily mean a low impact, as demonstrated in **Table 4**.

Table 4: Breach impact by Code obligation

Code obligation	No. of breaches	No. of customers impacted	Financial impact ($)
Provision of credit	4,178	12,988	1,160,270
Privacy and confidentiality	2,743	17,680	116,188
Debt collection	2,061	19,327	878
Internal dispute resolution	240	316	68
Staff training and competency	202	363	212,706
Financial difficulty	183	973	249,836
Direct debits	93	170	34,252
Electronic communications	76	75	0
Terms and conditions	60	100,869	795,390
Guarantees	36	69	435,210
Total	**9,872**	**152,830**	**3,004,798**

The financial impact data is problematic. One major bank reported zero financial impact for all breaches. Banks may be reporting zero financial impact where the customer suffered financial loss that was later fully remediated.

The CCMC will explore this reporting issue with banks and develop a more consistent approach. This will include clarifying whether banks are to report financial impact before or after remediation.

3.6 Monitoring

The CCMC also asked banks about how they monitor Code compliance. Encouragingly, banks' responses indicate that they have substantive monitoring programs and use a range of methods to identify and report on Code compliance. Across the industry, comprehensive call monitoring and quality assurance programmes are used to assess compliance and the quality of staff members' interactions with customers. The inquiry identified many good monitoring practices, which are detailed throughout the report.

However, the CCMC does have concerns about compliance teams' oversight of bank system testing. Across several of the monitoring areas assessed in this inquiry, banks provided minimal or no information about system testing.

Where banks rely on systems to fulfil their obligations to customers, the CCMC expects banks to test these systems regularly and comprehensively.

4 Provision of credit

To comply with the provision of credit obligation in clause 27 of the Code, banks are required to exercise the care and skill of a diligent and prudent banker in selecting the credit assessment method to apply to a credit facility or credit increase; applying the selected credit assessment method to the customer; and forming an opinion on the customer's ability to repay the credit facility.

4.1 Credit applications

In 2016–17 banks assessed 6,169,853 applications for credit.[4] Almost half (48%) of these concerned either credit cards (34.6%) or credit card limit increases (13.6%). The large majority of applications (93%) were for credit products for individual customers. Home loans accounted for about one-quarter of applications from individual customers, including 17% for owner-occupier home loans and 8% for investor home loans. Among small business customers, secured business loans were the most prevalent credit product, accounting for 65% of small business applications.[5]

4.2 Breach data

For this inquiry, banks reported 4,178 provision of credit breaches in 2016–17, a slight downwards revision from the 4,200 breaches reported in the 2016–17 ACS.

The products involved in most breaches were home loans (57%) and personal loans (27%). Despite the large number of credit card applications assessed by banks, credit cards accounted for just 12% of provision of credit breaches.

Table 5: Provision of credit breaches by product type

Product type	No. of breaches	% of breaches
Home loan	2,367	57%
Personal loan	1,148	27%
Credit card	489	12%
Business lending	50	1%
Multiple credit products	36	1%
Car loan	3	0.07%
Investment loan	1	0.02%
Personal overdraft	1	0.02%
Asset finance	1	0.02%
Construction loan	1	0.02%
Product type not recorded or specified	81	2%
Total	**4,178**	

[4] Applications for credit where the bank's assessment was completed (formally approved or declined) between 1 July 2016 and 30 June 2017.
[5] Some banks noted that their systems do not capture small business data using the Code's employee-based definition. As such, business lending data was often provided using banks' own internal classifications.

4.2.1 Key breaches

Most (92%) of the provision of credit breaches were a result of the following three types of incidents, all reported by a single bank:

Telephone information requests

A total of 2,577 or 62% of provision of credit breaches occurred where the telephone credit application process was not followed correctly because the staff member failed to collect all required information about the customer. The products that were the subject of these breaches were:

- home loans (1,603)
- personal loans (603)
- credit cards (371).

Debt consolidation discussions

Some 415 or 10% of provision of credit breaches occurred where discussions about consolidating debt were not conducted correctly. The products that were the subject of these breaches were:

- personal loans (412)
- home loans (2)
- credit cards (1).

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 that these breaches were unlikely to have any impact on customers. However, particularly given the volume of breaches, the CCMC is concerned that this assessment may not be accurate.

The CCMC expects that where a breach has been reported, the incidents will be fully investigated, tracked and monitored so that the bank can appropriately measure and manage any impact on customers. It will be following up with the bank directly.

Supporting documents

A total of 859 or 20% of provision of credit breaches occurred where documents did not match or support some elements of the credit application. The products that were the subject of the breaches were:

- home loans (695)
- credit cards (89), and
- personal loans (75).

Again, all of these breaches were caused by human error, where staff failed to follow the bank's process. These breaches were identified by the bank's credit quality assurance team. To correct the breaches, staff were given coaching and performance management.

The bank had not determined the full impact of the supporting documents breaches but noted that the files were placed on a 'watchlist' for 12 months so that if arrears were identified, the file could be reviewed before any collections activity was undertaken.

4.2.2 Other types of breaches reported by all banks

The remaining 327 breaches (8% of total provision of credit breaches) concerned a range of issues. In 266 cases, the lending decision was inappropriate, incorrect or 'not responsible' for one or more of the following reasons:

- the customer could not afford the credit repayments (94 breaches)
- the customer's financial situation was incorrectly calculated or recorded (55)
- the bank used incorrect or incomplete information in its lending decision (39)
- a credit check was not completed or completed incorrectly (31)
- the customer's situation was inappropriate for the credit provided, including for reasons related to age, health or financial situation (20)
- the information provided by the customer was not verified or not verified correctly (18)
- the bank did not make sufficient enquiries about the customer's needs or financial situation (6).

For most of these 266 breaches, banks did not confirm whether the breach meant a customer was given credit that they could not afford or whether the bank provided remediation to the customer. The CCMC encourages banks to include these details when reporting provision of credit breaches in future.

Other provision of credit issues included:

- a failure to pay out a customer's existing credit facility when opening the new credit facility (15 breaches)
- recommending, offering or providing an incorrect credit facility to the customer (14)
- system issues impacting credit applications (8).

4.2.3 Causes of breaches

The overwhelming majority (4,135 or 99%) of provision of credit breaches were caused by human error. Interestingly, however, banks attributed only four of these human error breaches to a training deficiency.

Six provision of credit breaches were caused by staff misconduct or fraud, and 12 by system errors. For another five breaches, the cause was not recorded. From the description of the incidents that led to these breaches, it seems they were the result of staff errors. Other causes included processing issues, which may involve human or systems errors.

As noted earlier, the CCMC expects banks to provide effective staff training and develop systems and controls that help to prevent human errors.

4.2.4 Identification of breaches

Almost three-quarters (72%) of breaches were identified through call monitoring.

Table 6: Methods of identifying provision of credit breaches

Identification method	Total
Call monitoring	2,993
Credit control/credit quality assurance	931
Internal quality assurance monitoring ('Line 1'[6])	146
Customer complaints	40
Self-identified and reported by staff member	27
Control testing of IT systems	14
Financial Ombudsman Service	14
Internal review team, including audit and fraud	11
Not recorded	2
Total	**4,178**

4.2.5 Corrective actions

In most cases, banks took multiple steps to correct and remediate provision of credit breaches. The main actions included one or more of the following:

- providing staff with further training, coaching or feedback (4,099 breaches)
- holding performance management or disciplinary discussions with staff members, including a small number of terminations and warnings – see below (3,861)
- enhancing monitoring or putting controls in place (886)
- refunding, reimbursing or otherwise compensating customers (63)
- correcting the issue (22)
- implementing a system fix (12)
- reviewing or improving processes (11)
- apologising to the customer (4)
- communicating or corresponding with the customer (3)
- deciding that the guarantee is unenforceable (1)
- providing financial difficulty monitoring/assessment/assistance (1).

Disciplinary action included warnings (3 breaches) and termination in fraud and other cases (3 breaches).

Again, banks' responses often focused on preventing reoccurrence of an incident or breach and did not address how irresponsible or inappropriate lending may have affected the customer.

[6] 'Line 1' is a reference to the three lines of defence model for risk and compliance management.

4.2.6 Customer impact

A total of 12,988 customers were impacted by the 4,178 provision of credit breaches.

Although nearly all provision of credit breaches affected one customer, there were notable exceptions. One bank reported three breaches that affected 8,653 customers in total. In the case of one breach that affected 6,200 customers, the bank failed to provide the correct notice period for an interest rate increase. Customers were refunded $235,000.

The CCMC has concerns that banks are not always fully exploring how breaches affect customers. Banks reported financial detriment for fewer than 1% of provision of credit breaches. The total financial impact of the 31 breaches reported by four banks was $1.16 million. In 3,851 cases, the banks reported that the financial impact was unknown and in 237 cases, they said there was no financial impact.

4.3 Monitoring

Banks appear to have robust frameworks for monitoring how credit applications are assessed, approved and declined. For the most part, banks' monitoring activities address the end-to-end manual credit application and fulfilment process, with files reviewed before and after the loan is approved and drawn down. Banks routinely monitor Code compliance and staff interactions with customers through call monitoring, quality assurance reviews and 'hindsight' reviews, which together accounted for almost all (97.4%) of the provision of credit breaches identified and reported (see Table 6 on page 17).

The CCMC was also pleased to see that many banks had adequate escalation and reporting of compliance with the Code, with many banks reporting that outcomes of monitoring reports are provided to Risk Committees or other senior bank staff. The CCMC considers that this kind of escalation and oversight from senior staff is a crucial part of achieving a positive compliance culture.

Overall, monitoring of the provision of credit obligations appeared to be the most structured and robust of all Code provisions examined in this inquiry. The CCMC also identified two particular instances of good practice in one bank's response.

Good practice

Whereas many banks increase their scrutiny of staff who are underperforming, one bank reported that it also conducts additional monitoring of staff with the highest sales. This added oversight allows it to address any concerns with sales behaviour.

This bank also reported strong engagement between its Compliance and Internal Dispute Resolution teams, who meet regularly to discuss trends and concerns about provision of credit.

Nevertheless, the industry did not always provide enough information to demonstrate robust monitoring. In its 2017 Provision of Credit Inquiry[7], the CCMC noted that many credit decisions are made, at least in part, by automated processes. This is not dissimilar to the provision of secured credit, where banks report that they rely on systems to provide credit scoring, among other things. Most banks provided little information about any proactive testing of these automated credit assessment systems. This is of great concern to the CCMC and will be raised with the industry directly.

In addition, two banks reported practices that were of concern to the CCMC. One bank reported that it monitors one phone call per staff member per month. This is significantly out-of-step with the many other banks who reported that at least four calls are monitored. In the CCMC's opinion, monitoring one phone call per staff member per month is insufficient. The CCMC will raise this feedback with the relevant bank directly.

Similarly, a different bank reported that its monitoring program was specifically designed to target medium- and high-risk loans, stating that as its 'minimum standards' did not require it to test low-risk products, it did so only on an 'ad hoc' basis as part of thematic reviews.

The CCMC reminds banks that clause 27 of the Code requires them to act as a prudent and diligent banker when selecting and applying the credit assessment methods and when forming an opinion on the customers' ability to pay. This obligation is owed to a customer regardless of whether the product is low- or high-risk. The CCMC will discuss this approach with the individual bank directly.

The CCMC expects banks' monitoring to be comprehensive. Monitoring should be end-to-end, incorporating any offshore processing hubs and other third parties. It should include proactive monitoring of systems responsible for any part of the credit decisioning process. Finally, it should employ a variety of robust monitoring activities focused on both prudential obligations and obligations to customers. Monitoring outcomes should then be reported and escalated to senior staff.

[7] CCMC, http://www.ccmc.org.au/cms/wp-content/uploads/2017/01/CCMC-Inquiry-Report-Provision-of-credit-January-2017.pdf, January 2017

5 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. The Code also sets out obligations relating to how the guarantee is signed and how guarantors can withdraw from a guarantee.

5.1 Securing credit facilities with a guarantee

Banks reported that more than 180,000 credit applications approved and finalised in 2016–17 were secured by a guarantee. Across the industry, guarantees secure between around 3% and 10% of lending. There is wide variation among banks in the extent to which guarantees are used to secure lending. Individual banks reported that as few as 0.03% or as many as 75% of their credit accounts were secured by a guarantee as at 30 June 2017. The percentage of loans secured by a guarantee is influenced by the product range offered by the bank.

Guarantees appear to be more common in business lending than consumer lending. When used in consumer lending, they tend to be provided for home loans.

5.2 Breach data

In the inquiry, the number of guarantees breaches was revised to 36, down from the 44 reported in the ACS. The CCMC considers that a further two of these 36 cases may not be Code breaches, and it will discuss these directly with the banks involved.

5.2.1 Types of breaches

For 15 of the breaches, the bank did not give the guarantor until the next day to consider the guarantee (as required under clause 31.5b). Most (16) of the rest of the breaches occurred where banks did not provide appropriate notices and information to the potential guarantor, or did not have evidence that they had done so.

5.2.2 Causes of breaches

More than 85% of guarantees breaches were attributed to human error.

5.2.3 Identification of breaches

Half of all guarantees breaches were identified through 'Line 1' quality assurance monitoring or internal review. The remaining breaches were identified through other proactive monitoring activities or as a result of a customer complaint or notification.

Table 7: Methods of identifying guarantees breaches

Identification method	No. of breaches
'Line 1' quality assurance monitoring or internal review	18
Customer complaint	9
Self-reported by staff member	3
Financial Ombudsman Service	2
Credit control/credit quality assurance	2
Customer notified bank	1
Unknown (not recorded in bank's risk and compliance system)	1
Total	**36**

5.2.4 Corrective actions

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

- provided staff with further training, coaching or feedback (22 breaches)
- did not enforce the guarantee (7)
- corrected the issue, including sending required information to the guarantor (6)
- provided the customer with refund or goodwill payment (2)
- provided 'consequence' or performance management for the staff member involved (2)
- enhanced monitoring or controls (2)
- apologised to the customer (1)
- implemented a system fix or reviewed and/or improved processes (1).

For one breach, no corrective action was needed.

In many cases, the remedial action focused on ensuring that the incident did not occur again. While this is positive, when correcting and reporting on a guarantees Code breach, the CCMC also expects banks to reflect the standing of a guarantee.

5.2.5 Customer impact

The 36 guarantees breaches impacted 69 customers and had a total financial impact of about $435,000.

5.3 Monitoring

Banks' report that that monitoring activities to ensure compliance with Guarantee provisions is largely undertaken as part of the provision of credit monitoring framework at the pre-settlement or fulfilment stage of the loan.

Good practice

One bank reported that it requires a checklist to be completed and recorded when pre-contractual documents are both issued and received. This additional step ensures that requirements for the pre-contractual provision of documents are satisfied.

6 Debt collection and financial difficulty

Banks must try to help customers overcome their financial difficulties with any credit facility they have with their bank. Under clause 28 of the Code banks are also required to assist customers in financial difficulty by:

- dealing with the customer's authorised financial counsellor or representative
- considering contacting customers who the bank identifies as potentially experiencing difficulties
- informing the customer about the National Credit Code
- taking available information about a customer's financial situation into account when determining whether or not they are able to provide assistance
- providing, in writing, the bank's decision about any financial difficulty assistance, including the reasons for the decision and the main details of the arrangements.

These financial difficulty obligations overlap considerably with banks' debt collection obligations, set out in clause 32 of the Code:

- 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.

6.1 Debt collection and financial difficulty data

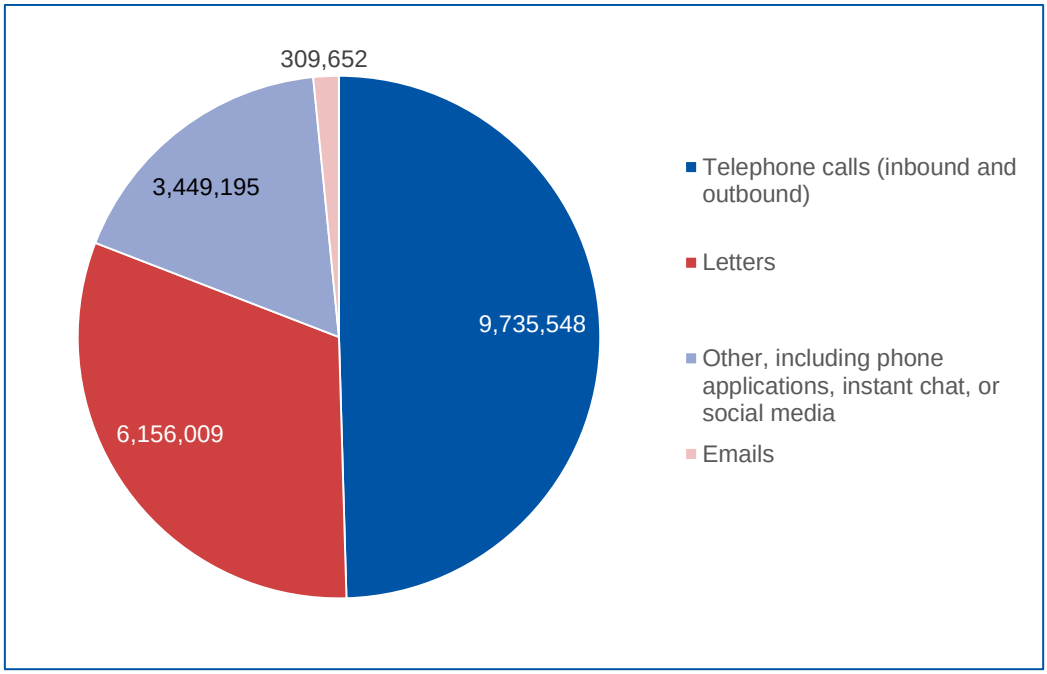
The CCMC asked banks how many:

- accounts and/or customers were subject to debt collection activities
- successful contacts[8] were made between customers and the bank's debt collection and financial difficulty teams.

Although banks interpreted terms differently and were sometimes unable to extract the required information, they provided data with some broad indicative value. During 2016–17 debt collection activity was conducted on 9.48 million accounts, incorporating more than 30.5 million successful contacts with customers. The breakdown of contact types is shown in Chart 2.

[8] Contacts was broadly defined to mean where there has been a direct interaction or communication between the bank and the customer. The CCMC acknowledges that the term 'contacts' can be interpreted differently and referred banks to Part 2, Section 3 of the *ACCC/ASIC Debt Collection Guideline* for further information.

Chart 2: Breakdown of debt collection contacts



There were more than 1.6 million contacts between customers and the banks' financial difficulty teams, and through these, customers lodged more than 300,000 requests for financial difficulty assistance. About three-quarters (73%) of these requests were granted (Table 8).

Table 8: Financial difficulty data

Total contacts	Requests for financial difficulty assistance received	Requests for financial difficulty assistance granted	% of requests granted
1,641,765	303,635	220,627	73

6.2 Breaches

In the inquiry, the number of debt collection breaches was revised substantially upwards, increasing from 1,119 in the ACS to 2,061 in the inquiry. This increase was the result on one bank reporting details of an additional 945 debt collection breaches. This bank accounts for the vast majority (96%) of debt collection breaches. More than three-quarters (77%) of debt collection breaches related to incomplete or incorrect file notes (Table 9).

Table 9: Types of debt collection breaches

Type of incident	No. of breaches	% of breaches
Incomplete or inaccurate file notes	1,579	77%
Incorrect information provided in arrangement negotiations or misrepresentation of consequences	160	8%
Unnecessary contact with customers	100	5%
Frequency/number of contacts guidelines not met	51	2%

Improper collections activity	26	1%
Complaint not managed correctly	25	1%
Incorrect contact with a represented customer	17	1%
Failure to follow agreed payments	14	1%
Potential financial difficulty triggers not identified and/or followed up	15	1%
Collection activity while financial difficulty assistance being considered or repayment arrangement is in place	11	1%
Collection activity while payment arrangement in place	8	0.4%
Default notice or listing error	8	0.4%
Other	47	2%
Total	**2,061**	

In contrast to debt collection breaches, the number of financial difficulty breaches was revised downwards from 207 in the ACS to 183 in the inquiry. The main types of financial difficulty breaches were:

- potential financial difficulty triggers not being identified and/or followed up
- financial difficulty assistance requests not being actioned or responded to within required timeframes.

Table 10: Types of financial difficulty breaches

Type of incident	No. of breaches	% of breaches
Potential financial difficulty triggers not identified and/or followed up	70	39%
Financial difficulty assistance request not actioned/responded to within timeframe	55	31%
Incorrect correspondence/information provided to customer	10	6%
Debt collection activity while financial difficulty assistance being considered or an arrangement is in place	10	6%
Financial difficulty assistance request not processed correctly or genuinely considered	9	5%
Failure to advise customer of financial difficulty options	6	3%
Improper collections activity	3	2%
Default notice or listing error	2	1%
Failure to follow agreed payment instructions	2	1%
Response to financial difficulty assistance request not sent	2	1%
Other	9	5%
Total	**178**[9]	

There is some overlap between debt collection and financial difficulty Code breaches. Some of the breaches shown in Tables 9 and 10 apply to both sets of provisions:

[9] There were five additional financial difficulty breaches reported by one bank where the information provided to the CCMC indicated that they may not have been a breach of the financial difficulty obligations under the Code. The CCMC will discuss this with the bank involved.

- collection activity while financial difficulty assistance was being considered or a repayment arrangement was in place
- default notice or listing error
- potential financial difficulty triggers not being identified and/or followed up.

6.2.1 Causes of breaches

Human error was listed as a cause of 98% of debt collection breaches and 84% of financial difficulty breaches, with banks confirming that in many cases this was because a process was not followed. Systems errors accounted for a further 30 debt collection breaches and 11 financial difficulty breaches.

6.2.2 Identification of breaches

Some 88% of debt collection breaches and 28% of financial difficulty breaches were identified through call monitoring activities. Another 22 debt collection breaches and 29 financial difficulty breaches were identified through complaints processes. Most other debt collection and financial difficulty breaches were identified through 'Line 1' quality assurance.

6.2.3 Corrective actions

The banks undertook one or more of the following corrective actions for most debt collection breaches:

- provided staff training, coaching or feedback (1,055 breaches)
- apologised to the customer (102)
- corrected details (such as removing default notices) (176)
- provided financial difficulty assistance or assessed an assistance request (30)
- implemented a system fix (24).

For 838 breaches (mostly one bank that reported file notes issues), remedial actions were not recorded in the bank's incident management system. The CCMC is concerned by this and will discuss the matter with the bank involved.

Remedial actions for financial difficulty breaches included:

- providing staff training, coaching or feedback (65 breaches)
- providing financial difficulty assistance or assessing an assistance request (45)
- enhancing the bank's monitoring and controls (15)
- providing the customer with refund or goodwill payment (14).

In 38 breaches related to identifying financial difficulty triggers, the bank did not provide details of corrective measures taken. The CCMC considers it is crucial that where these issues are identified, the bank considers whether and how it should discuss the customer's situation (in accordance with clause 28.4 of the Code), and records this information.

6.2.4 Customer impact

Debt collection and financial difficulty breaches often affect multiple customers (Table 11).

Table 11: Customer impact of financial difficulty and debt collection breaches

	No. of breaches	No. of customers impacted
Debt collection	2,061	19,327
Financial difficulty	183	973

6.3 Monitoring

After rising steadily for three consecutive years, banks' breaches of debt collection obligations increased a further 160% in the 2016–17 reporting period. Keen to better understand this increase, the CCMC sought information from banks about their debt collection compliance monitoring programs.

Generally, banks reported taking similar monitoring approaches, conducting call monitoring, quality assurance reviews and 'hindsight' reviews. Banks generally have robust processes to monitor interactions with customers, monitoring an average of four or five calls per staff member per month.

However, the CCMC has a number of concerns about how banks monitor their compliance with debt collection obligations. As banks' debt collection and financial difficulty teams often overlap, these concerns extend to financial difficulty monitoring.

The CCMC again noted a lack of information about proactive testing of debt collection systems, such as dialler systems or case management systems. Similarly, banks failed to provide sufficient information about how financial difficulty systems are monitored.

Nor did banks provide sufficient information about any monitoring of customer correspondence such as letters, emails and SMS messages. Such correspondence was recently the cause of a long-running breach with a wide customer impact (see the case study below). Noting this, the CCMC reminds banks that both standard and bespoke debt collection and financial difficulty letters should be reviewed regularly for Code and regulatory compliance.

Case Study

In November 2016, the CCMC received an allegation from a community legal centre that a bank had breached the Code's debt collection obligations. After a financial difficulty arrangement had been agreed, the bank issued a standard form letter that threatened continued debt collection activity.

Acknowledging the breach, the bank reported that over a three-year period, it had sent the letter to all recipients of financial difficulty assistance across all retail product lines – impacting upwards of 70,000 customers. The bank has now corrected the letter.

Finally, the CCMC also has concerns about banks' oversight of third party collection agents. Only one bank provided substantial information about how it monitors third party compliance, which is required under Code clause 32.1.

The CCMC is interested in how banks ensure compliance with a unique Code clause that requires banks to give genuine consideration to a customer's application for financial difficulty assistance and try and help a customer to overcome their financial difficulties. The CCMC will examine this issue as part of its in-depth inquiry into banks' compliance with their financial difficulty obligations, on which the CCMC expects to report in September 2018.

7 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.

7.1 The CCMC's focus on direct debits

Due to ongoing non-compliance, banks' direct debit obligations have been a focus of the CCMC's monitoring for many years. The CCMC first highlighted these issues in 2008, with mystery shopping research finding that in 80% of contacts, bank staff were providing incorrect and non-compliant advice to customers enquiring about cancelling a direct debit. Follow-up research in 2010, 2011 and 2017 revealed that compliance was not sufficiently improved.

In its 2017 report,[10] the CCMC reported that seven banks provided data showing that, collectively, an average of more than 15,500 direct debit cancellation requests were received each month. However, the CCMC considered that the actual number received across the industry was significantly greater. While cancellations requests were low relative to the more than 50 million direct debit transactions made each month, even a low non-compliance rate can impact many customers.

In the inquiry, banks reported 93 direct debit breaches, two fewer than the 95 reported in the ACS. However, the CCMC has previously raised concerns about whether banks' monitoring processes are sufficiently robust to identify and report on breaches of direct debit obligations. As such, the CCMC will continue to monitor compliance through mystery shopping and the ACS program.

7.2 Breach data

Most direct debit breaches concerned a bank's failure to cancel or amend a direct debit at a customer's request.

Table 12: Types of direct debit breaches

Type of breach	No. of breaches	% of breaches
Customer request to cancel direct debits not actioned	59	63%
Customer request to cancel/amend direct debits not actioned	19	20%
Direct debit set up incorrectly	4	4%
Complaint not actioned correctly or promptly	4	4%
Direct debit payments incorrectly processed	2	2%
Customer provided incorrect direct debit cancellation information	1	1%
Bank cannot cancel direct debit	1	1%

[10] CCMC, http://www.ccmc.org.au/cms/wp-content/uploads/2017/10/CCMC-Report-Improving-banks%E2%80%99-compliance-with-direct-debit-cancellation-obligations-October-2017.pdf, October 2017

Bank cannot cancel direct debit and customer should contact the merchant	1	1%
Complaint not actioned correctly or promptly	1	1%
Delay in processing direct debit	1	1%
Total	**93**	

Based on the information provided, a small number of direct debit breaches that were reported may not have been a breach the Code. For example, errors in processing direct debits alone are unlikely to be a breach unless there has been an associated complaint that has not been dealt with appropriately.

7.2.1 Causes of breaches

All but one direct debit breach was caused by human error. The remaining breach was a system error where direct debit payments were incorrectly processed, affecting 50 customers. However, this processing error may not constitute an actual breach.

7.2.2 Identification of breaches

While breaches of most Code obligations are predominantly identified through banks' proactive monitoring activities, most direct debit breaches (72) were identified as a result of customer complaints. The remainder were mostly identified through banks' quality assurance. One breach was reported as a result of the CCMC's monitoring activities.

In its 2017 direct debits report, the CCMC made two recommendations to improve breach identification in this area. The CCMC expects that the implementation of those recommendations will lead to improved monitoring of the direct debits obligations.

7.2.3 Corrective or remedial actions

For each breach, banks took one or more of the following actions:

- corrected the issue, typically by cancelling the direct debit (79)
- provided staff with further training, coaching or feedback (79)
- provided the customer with a refund or goodwill payment (56)
- apologised to the customer (44)
- implemented a system fix or improvement (2)
- reviewed and/or improved processes (2)
- enhanced monitoring or controls (1).

7.2.4 Customer impact

Some 170 customers were impacted by direct debit breaches, with a total financial impact of $34,252. However, based on its other monitoring activities, the CCMC believes that direct debit breaches often go unidentified and unreported. Therefore, the true customer impact is likely to be greater.

8 Terms and conditions

The terms and conditions (T&Cs) obligations under clause 12 of the Code require banks to provide, on request, the T&Cs, full particulars of standard fees and charges and particulars of the interest rates applicable for any ongoing banking service they offer. The Code also sets out what information the T&Cs should contain, how they should be written and when they should be provided. Banks are required to include a statement that the relevant provisions of the Code apply to the banking service.

8.1 Breach data

The number of T&Cs breaches reported in the inquiry was 60, a downwards revision from the 65 breaches reported in the ACS[11].

T&Cs breaches fall into two categories:

- issues with content or provision of the T&Cs (75%)
- non-compliance with the T&Cs (about 25% of breaches).

Examples of non-compliance with second category include:

- customers not receiving the correct amount of interest on a savings product
- a fee being charged monthly rather than six-monthly
- a fee not being waived when it should have been
- incorrect payment amounts being set up, leading to additional interest and collections activities
- incorrectly charging a foreign currency fee on debit card transactions with certain merchants
- settling loans as principle and interest instead of interest only
- loyalty bonuses or discounts not being received
- offset accounts not being linked.

The CCMC considers that many of the above examples would be better reported under another category of Code obligations: key commitments (clause 3). Such errors do not necessarily breach the Code's T&Cs obligations where the T&Cs have the correct content and were provided appropriately.

This miscategorisation is particularly significant given the wide customer impact of reported T&Cs breaches. T&Cs breaches affected 100,869 customers, far more than the number of customers affected by breaches in any other area. Moreover, while only one-quarter of T&Cs breaches concerned non-compliance with T&Cs, these breaches accounted for more than 80% of the customer impact of T&Cs breaches.

One T&Cs breach accounted for more than half of all the customers affected by the Code breaches reported in this inquiry. In this case, the bank incorrectly charged a foreign currency fee on debit card transactions with certain merchants between

[11] The T&Cs breaches covered in this section of the report excludes three breaches that one bank reported to the CCMC in detail through the 2016-17 ACS program.

2011 and 2016, when the bank implemented a system fix. This single breach affected some 80,000 customers with a combined financial impact of $680,000.

The total financial impact of the T&Cs breaches was $795,390.

8.1.1 Causes of breaches

System errors (15) and process deficiencies (7) played a larger role in T&Cs breaches than in other areas, although human error (35) was still the most common breach cause.

8.1.2 Identification of breaches

Staff members identified half (49%) of the T&Cs breaches, with about one-quarter (23%) identified through complaints.

Table 13: Identification of breaches

Identification method	No. of breaches
Staff member	28
Complaint	13
'Line 1' quality assurance monitoring	6
Internal review	4
Call monitoring	3
Quality assurance review by second line compliance	2
Information not provided by bank	1
Total	**57**

8.1.3 Corrective actions

The banks took one or more of the following corrective actions for each breach:

- corrected the issue that the breach related to, such as adjusting fees or updating incorrect T&Cs documentation (25 breaches)
- provided staff training, coaching or feedback (17)
- communicated or corresponded with the customer (16)
- implemented a system fix (15)
- provided the customer with refund or goodwill payment (14)
- enhanced monitoring or controls (4)
- apologised to the customer (2)
- reviewed processes and made improvements (2).

8.2 Monitoring

In describing how they monitor their compliance with T&Cs requirements, most banks focused primarily on the design and content of T&Cs documents. Sometimes this is part of the 'business as usual' process: for example, one bank

reported that when amending T&Cs following a price change, it reviews and signs off the whole document for its overall compliance. Banks also reported conducting periodic reviews of T&Cs.

Banks put less emphasis on reporting how they ensure that customers are issued with the correct T&Cs document. Where comments were made, banks reported that this monitoring is typically done through ‘hindsight’ reviews.

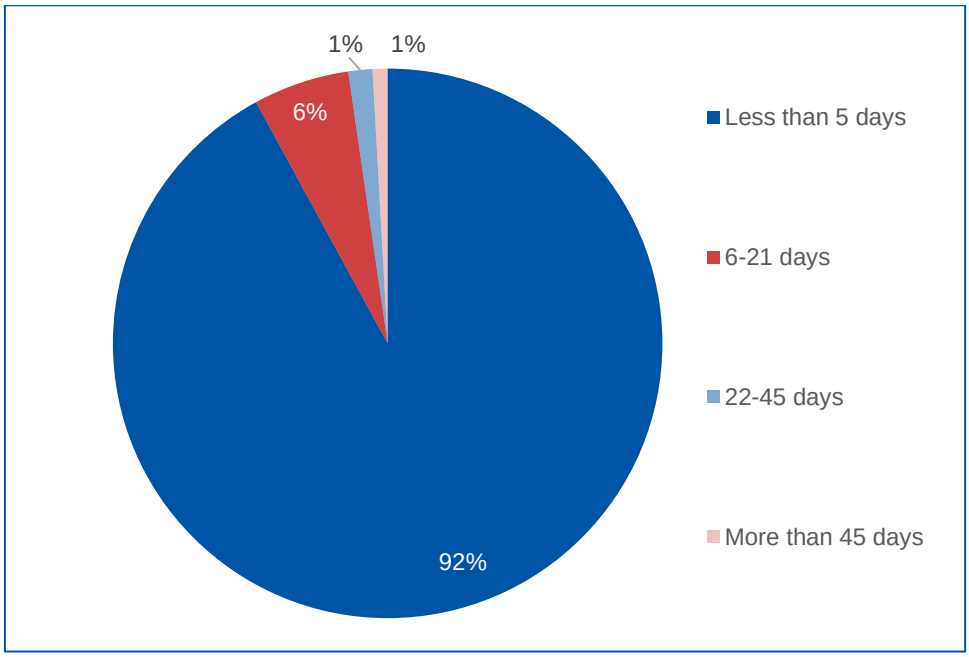
9 Internal dispute resolution

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 165*.

9.1 Complaints data

The CCMC collects complaints and IDR data through its ACS program each year. Banks resolved 1,205,253 complaints in 2016–17. Chart 3 shows how quickly complaints were resolved.

Chart 3: Complaint resolution 2016–17



9.2 Breach data

In the inquiry, banks revised the number of IDR breaches down to 240 from the 285 breaches reported in the ACS. The vast majority (95%) of breaches were reported by one bank.

It could be concluded that the low number of breaches compared with the high volume of complaints resolved indicates good compliance in this area. However, as the CCMC stated in its 2016–17 Annual Report, it is concerned that only five banks reported any IDR Code breaches. A number of banks, including major banks, reported very low or no breaches of IDR obligations.

9.2.1 Types of breaches

The vast majority of IDR breaches were due to a customer's dissatisfaction not being recognised and logged as a complaint (64%) or a final written response not being sent to the complainant (30%).

Table 14: Types of IDR breaches

Types of IDR breaches	No. of breaches
Customer's expression of dissatisfaction not recognised and logged as a complaint	153
Final response in writing not sent to complainant	73
Complaint progress letters not issued within required timeframes	4
Complaints not recorded	4
Complaints not recorded or actioned	3
Errors in the resolution letter	1
Bank did not respond within required timeframe	1
Complaint resolved incorrectly	1
Total	**240**

Most failures to log a complaint were reported by one bank. While these breaches make up a large proportion of total IDR breaches, they represent only a very small percentage of the complaints captured and recorded by that bank.

9.2.2 Causes of breaches

All IDR breaches were caused by human error. In the vast majority of cases (230 of 240 breaches or 96%), banks reported that this human error involved deviation from the bank's process. One breach was caused by insufficient training.

9.2.3 Identification of breaches

Most breaches were identified through call monitoring or QA activities.

9.2.4 Corrective actions

Banks took one or more of the following corrective actions:

- recorded and managed/resolved the complaint (229 breaches)
- provided staff with further training, coaching or feedback (10)
- held performance management discussions with staff (3)
- paid compensation to the customer (2).

9.2.5 Customer impact

The IDR breaches impacted 316 customers.

9.3 Monitoring

Banks generally reported that they monitor compliance with IDR obligations through a combination of call monitoring and quality assurance reviews. Of the 13 Code subscribing banks involved in this inquiry, six reported that they monitor between three and eight calls per staff member per month. One bank reported that

it reviews 100% of calls. Concerningly, however, five banks did not report on call monitoring activity or reported that they did not conduct call monitoring in IDR teams.

Many banks reported that they rely on a case management system to either issue letters or issue prompts to the staff member that an action is required. Further, many banks reported that they rely on these systems to generate reports on compliance numbers and trends. Consistent with the CCMC's findings for other Code obligations, only a few banks provided enough information to demonstrate that they are regularly testing these IDR systems.

The CCMC was pleased that several banks provided information about how they escalate and report complaints to senior staff. Several banks described related meetings or calibration sessions. For instance, one bank reported that it conducts monthly forums discussing complaint issues and trends, with forum outcomes then disseminated to various business units. This bank's compliance report is issued to its senior leadership group and its Risk and Compliance Committee.

10 Privacy and confidentiality

The privacy and confidentiality obligations under clause 24 of the Code state that the bank acknowledges that, in addition to its duties under the *Privacy Act 1988*, it has a duty of confidentiality towards its customers, except where:

- disclosure is compelled by law
- there is a duty to the public to disclose
- its interests require disclosure
- disclosure is made with the customer's express or implied consent.

10.1 Breach data

In the inquiry, banks revised the number of privacy and confidentiality breaches to 2,743, fewer than the 2,779 reported earlier in the ACS. Identification errors and information provided or disclosed to an incorrect party were the main breach types, respectively accounting for 31% and 29% of privacy and confidentiality breaches. Tax File Number issues also contributed 18% of breaches (Table 15).

Table 15: Types of breaches

Type of incident (total for type)	Sub-category	No. of breaches	% of breaches
Identification errors (852)	Caller not correctly identified/no attempt to identify caller	819	31%
	Customer not successfully identified before continuing with the lending discussion	16	
	Further details not provided by bank	15	
	Failure to appropriately identify customer during inbound call	2	
Information provided or disclosed to incorrect party (801)	*Further details not provided by bank*	580	29%
	Email	117	
	Letter	40	
	Card	38	
	Statement	20	
	Other	6	
Tax File Number (TFN) issues (491)	TFN not removed	484	18%
	TFN applied to account without customer permission	5	
	Further details not provided by bank	2	
Credit bureau/reference check issues (151)	Credit check without customer consent	142	6%
	Other	9	
Incorrect linking of accounts		127	5%
Privacy policy scripting not read/not disclosed		100	4%
Other		221	8%
Total		**2,743**	

10.1.1 Causes of breaches

The vast majority (98%) of privacy and confidentiality breaches included human error as a cause. Some 57 breaches were at least partly a result of a system error.

10.1.2 Identification of breaches

Most of the privacy and confidentiality breaches were identified through call monitoring and other QA activities. More than 400 breaches were identified as a result of a customer complaining or informing the bank.

10.1.3 Corrective or remedial actions

For more than half of all privacy and confidentiality breaches (1,667), concerningly information on corrective actions was not provided. For the remaining 1,076 breaches, the banks undertook one or more of the following corrective actions:

- provided staff training, coaching or feedback (684 breaches)
- corrected the issue (311)
- apologised to the customer (149)
- requested that the information to be destroyed, deleted or returned (138)
- communicated or corresponded with the customer (119)
- corrected or updated details (91)
- enhanced monitoring or controls (88)
- reviewed process and/or made improvements (68)
- held performance management or disciplinary discussions with staff (including warnings and termination in some rare cases) (66).

10.1.4 Customer impact

The privacy and confidentiality breaches impacted 17,680 customers, with a total financial impact of $116,188.

11 Staff training and competency

Under clause 9 of the Code, a bank will ensure its staff (and authorised representatives) are trained to understand the Code and its application, and to competently and efficiently discharge their functions.

A bank's compliance with the Code rests on the knowledge and skill of its staff. Staff who are trained in the Code are more likely to meet their obligations and recognise any non-compliance by others. The training obligations in the Code are therefore crucial. The CCMC expects banks to train staff to competently and efficiently discharge their obligations.

11.1 Breach data

Banks reported 202 staff training breaches in the inquiry, fewer than the 213 breaches recorded in the ACS.

Most staff training and competency breaches (173) are 'general' staff errors, and training is not specifically referenced. These include:

- processing errors (115)
- providing incorrect, inappropriate and/or conflicting information to a customer (43)
- privacy issues (9)
- acting without a customer's consent (4)
- not dealing with a complaint correctly or promptly (2).

The remaining staff training and competency breaches (29) occurred where staff performed their role without completing necessary or mandatory training.

Banks have different views about what constitutes a breach of this Code obligation. One bank takes a broad approach. 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. This bank accounts for more than 50% of reported staff training breaches. 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.

As part of the transition to the new Code of Banking Practice, the CCMC will consider this issue and provide guidance to banks on how they should approach breach reporting for staff training issues.

11.1.1 Causes of breaches

The vast majority (96%) of staff training breaches were due to human error.

11.1.2 Identification of breaches

Half of the staff training breaches were identified via customer complaints, and about one-fifth (20%) through call monitoring and quality assurance.

11.1.3 Corrective or remedial actions

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

- provided the customer with a refund, goodwill payment and/or waived a fee (99 breaches)
- provided staff training, coaching or feedback (99)
- apologised to the customer (79)
- corrected the issue (34)
- communicated or corresponded with the customer (6)
- enhanced monitoring or controls (3)
- implemented a system fix (2)
- held performance management discussions with staff (including warnings) (3)
- reviewed processes and made improvements (1).

11.1.4 Customer impact

Some 363 customers were impacted by the staff training breaches, with a total financial impact of $212,706.

11.2 Monitoring

Banks' approach to monitoring reflects their different interpretations of what constitutes a staff training and competency breach. Most banks reported monitoring staff members' completion of training. For example, one bank noted that a Code breach is recorded if mandated training is not completed when required. Another bank noted that a Code breach is recorded if a direct connection is made between staff performance and a gap in training.

Banks generally provided little information about the outcomes or consequences of non-compliance with staff training and competency obligations. Similarly, banks provided little information about whether staff who are non-compliant with *Regulatory Guide 146* training requirements are prevented from performing advisory and sales functions.

Notwithstanding these apparent gaps in information, evidence of good industry practice was included in one bank's response. This bank reported that non-compliance feeds into staff performance plans and that internal guidelines on remuneration impacts are available to line managers.

12 Electronic communications

Clause 35 of the Code states:

If a legislative electronic communications regime also applies to any information which this Code requires us [a bank] to provide (by writing or other means) we may provide you [a customer] with that information by electronic communication in accordance with that regime. Otherwise, provided it is not prohibited by legislation, we may provide this information to you consistently with the requirements for electronic communications specified in the ePayments Code (regardless of whether that code applies to the communication).

12.1 Breach data

Only one bank reported breaches of the electronic communications clause.

Two types of incident were reported: one which represented 75 breaches and impacted 75 customers and the other which represented one 'systemic breach' where the number of customers impacted is unknown.

In the first type of incident, mandatory scripting was not read to customers to obtain consent for online statements. These breaches were caused by staff failing to follow the scripting and/or processes, and were identified by call monitoring ('Line 1'). The bank's corrective action was to switch customers to paper statements.

In the second type of incident, online banking inbox messages and emails were not generated to customers advising that statements were available due to a system error. The error, which caused statement notifications not to be issued as required, was identified through an internal review. The error was corrected and statements reissued.

13 Appendix 1: Inquiry questionnaire

The following questionnaire was distributed to banks on 7 February 2018, with responses due by 29 March 2018.

Data was requested for the period 1 July 2016 to 30 June 2017 unless otherwise stated. With the exception of the breach details tables, the CCMC asked banks to provide a response to all questions regardless of whether or not the bank reported breaches of the Code obligation each question relates to in the 2016–17 ACS.

1. Provision of credit (clause 27)

1.1. If the bank reported any provision of credit breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table consisted of the following fields:

- Number of breaches
- Description of incident
- Product type
- Cause of breach
- Breach identification method
- Corrective/ remedial actions
- Number of customers impacted
- Total financial impact on customer(s)
- Other comments

1.2. Please complete the table below by providing the number of applications for credit where the bank's assessment was completed between 1 July 2016 and 30 June 2017.

The table consisted of the following fields:

- Product type
- Number of applications (individual customers)
- Number of applications (small business customers)
- Total number of applications

1.3. The CCMC is seeking information about the type and amount of monitoring conducted by the bank to support compliance with the provision of credit Code obligations between 1 July 2016 and 30 June 2017. Please use the questions below as a guide to providing this information. If the specific wording does not reflect the terms used by the bank or its approach to Code monitoring, please provide any additional or different information along with an appropriate explanatory note.

1.3.1. Please provide a summary of the monitoring methods that were in place between 1 July 2016 and 30 June 2017, including:

- a description of the actions
- who/what performs the actions (role(s)/type of system)
- how the actions are performed
- how regularly the action is performed, and
- why the action is performed

for each type of monitoring activity.

1.3.2. Please provide details about the amount of monitoring undertaken by the bank relating to applications for credit assessed, approved and declined between 1 July 2016 and 30 June 2017, for example:

- The number or percentage of applications on which a monitoring review was conducted before the credit application was finalised and funds were actually provided or drawn down.
- The number or percentage of applications on which a monitoring review was conducted after the credit application was finalised and funds were actually provided or drawn down.
- The number or percentage of telephone calls made or received about a credit application that were subject to a quality assurance review.
- The number or percentage of applications reviewed where the application was assessed in full by an automated process.
- Any reporting and monitoring conducted on an automated or partly-automated system or tool associated with the provision of credit.
- Whether any additional, exceptional or targeted monitoring or reviews were conducted.
- Any monitoring conducted by the bank's third line of defence or internal audit function.

2. Privacy and confidentiality (clause 24)

2.1. If the bank reported any privacy and confidentiality breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

3. Debt collection (clause 32)

3.1. If the bank reported any debt collection breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

3.2. How many accounts and/or customers were subject to debt collection activities by the bank during 2016–17?

3.3. How many successful contacts were there between customers and the bank's debt collection team in 2016–17? The CCMC acknowledges that the term

'contacts' is interpreted widely and refers the bank to Part 2, Section 3 of the ACCC/ASIC Debt Collection Guideline for further information. Please breakdown the bank's response to cover the following types of contact:

- telephone calls (inbound and outbound)
- letters
- emails
- SMS
- other, including phone applications, instant chat, or social media.

3.4. The CCMC is seeking information about the type and amount of monitoring conducted by the bank to support compliance with the debt collection Code obligations between 1 July 2016 and 30 June 2017. Please use the questions below as a guide to providing this information. If the specific wording does not reflect the terms used by the bank or its approach to Code monitoring, please provide any additional or different information along with an appropriate explanatory note.

3.4.1. Please provide a summary of the monitoring methods that were in place between 1 July 2016 and 30 June 2017, including:

- a description of the actions
- who/what performs the actions (role(s)/type of system)
- how the actions are performed
- how regularly the action is performed, and
- why the action is performed

for each type of monitoring activity.

3.4.2. Please provide details about the amount of monitoring undertaken by the bank relating to the Code's debt collection obligations between 1 July 2016 and 30 June 2017, for example:

- The number or percentage of accounts in debt collection where a quality assurance review was conducted.
- The number or percentage of debt collection telephone calls that were subject to a quality assurance review.
- The number or percentage of debt collection emails or other correspondence that were subject to a quality assurance review.
- Any reporting and monitoring conducted on the bank's processes/procedures or IT systems associated with debt collection.
- Whether any additional, exceptional or targeted monitoring or reviews were conducted.
- Any monitoring conducted by the bank's third line of defence or internal audit function.

4. Internal dispute resolution (clause 37)

4.1. If the bank reported any internal dispute resolution breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

4.2. The CCMC is seeking information about the type and amount of monitoring conducted by the bank to support compliance with the internal dispute resolution Code obligations between 1 July 2016 and 30 June 2017. Please use the questions below as a guide to providing this information. If the specific wording does not reflect the terms used by the bank or its approach to Code monitoring, please provide any additional or different information along with an appropriate explanatory note.

4.2.1. Please provide a summary of the monitoring methods that were in place between 1 July 2016 and 30 June 2017, including:

- a description of the actions
- who/what performs the actions (role(s)/type of system)
- how the actions are performed
- how regularly the action is performed, and
- why the action is performed

for each type of monitoring activity.

4.2.2. Please provide details about the amount of monitoring undertaken by the bank relating to internal dispute resolution between 1 July 2016 and 30 June 2017, for example:

- The number or percentage of complaints where a quality assurance review was conducted.
- How the bank monitored that complaints resolved at the first point of contact were resolved to the customer's 'complete satisfaction'.
- How the bank monitored that complaints resolved within 5 business days were resolved to the customer's 'complete satisfaction'.
- The level of monitoring of telephone calls, emails or any other correspondence that was undertaken.
- Any reporting and monitoring conducted on the bank's processes/procedures or IT systems associated with internal dispute resolution.
- Whether any additional, exceptional or targeted monitoring or reviews were conducted.
- Any monitoring conducted by the bank's third line of defence or internal audit function.

5. Staff training and competency (clause 9)

5.1. If the bank reported any staff training and competency breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

5.2. Please describe the bank's current approach to identifying, recording and reporting breaches of the staff training obligations. Please provide examples of the type of conduct or incident that banks would and would not consider to be a breach of the Code in this area.

5.3. Please outline any monitoring activities conducted by the bank to specifically review the bank's compliance with the staff training and competency obligations during the 2016–17 period.

6. Financial difficulty (clause 28)

6.1. If the bank reported any financial difficulty breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

6.2. How many successful contacts were there between customers and the bank's financial difficulty team in 2016–17? The CCMC acknowledges that the term 'contacts' is interpreted widely and refers the bank to Part 2, Section 3 of the ACCC/ASIC Debt Collection Guideline for further information. Please breakdown the bank's response to cover the following types of contact:

- telephone calls (inbound and outbound)
- letters
- emails
- SMS
- other including phone applications, instant chat, or social media.

6.3. The CCMC is seeking information about the type and amount of monitoring conducted by the bank to support compliance with the financial difficulty Code obligations between 1 July 2016 and 30 June 2017. Please use the questions below as a guide to providing this information. If the specific wording does not reflect the terms used by the bank or its approach to Code monitoring, please provide any additional or different information along with an appropriate explanatory note.

6.3.1. Please provide a summary of the monitoring methods that were in place between 1 July 2016 and 30 June 2017, including:

- a description of the actions
- who/what performs the actions (role(s)/type of system)
- how the actions are performed
- how regularly the action is performed, and
- why the action is performed

for each type of monitoring activity.

6.3.2. Please provide details about the amount of monitoring undertaken by the bank relating to financial difficulty between 1 July 2016 and 30 June 2017, for example:

- The number or percentage of accounts/ customers experiencing financial difficulty where a quality assurance review was conducted.
- The number or percentage of telephone calls related to financial difficulty that were subject to a quality assurance review.
- The number or percentage of emails or other correspondence related to financial difficulty that were subject to a quality assurance review.

- Any reporting and monitoring conducted on the bank's processes/procedures or IT systems associated with financial difficulty.
- Whether any additional, exceptional or targeted monitoring or reviews were conducted.
- Any monitoring conducted by the bank's third line of defence or internal audit function.

7. Direct debits (clause 21)

7.1. If the bank reported any direct debits breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

8. Electronic communications (clause 35)

8.1. If the bank reported any electronic communications breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

9. Terms and conditions (clause 12)

9.1. If the bank reported any terms and conditions breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

9.2. The CCMC is seeking information about the type and amount of monitoring conducted by the bank to support compliance with the terms and conditions Code obligations between 1 July 2016 and 30 June 2017. Please use the questions below as a guide to providing this information. If the specific wording does not reflect the terms used by the bank or its approach to Code monitoring, please provide any additional or different information along with an appropriate explanatory note.

9.2.1. Please provide a summary of the monitoring methods that were in place between 1 July 2016 and 30 June 2017, including:

- a description of the actions
- who/what performs the actions (role(s)/type of system)
- how the actions are performed

- how regularly the action is performed, and
- why the action is performed

for each type of monitoring activity.

9.2.2. Please provide details about the amount of monitoring undertaken by the bank relating to the terms and conditions obligations under the Code between 1 July 2016 and 30 June 2017, for example:

- Any quality assurance reviews conducted.
- Whether any additional, exceptional or targeted monitoring or reviews were conducted.
- Any monitoring conducted by the bank's third line of defence or internal audit function.

10. Guarantees (clause 31)

10.1. If the bank reported any guarantees breaches in the 2016–17 ACS, please complete the table below. Where the nature, cause and outcome of more than one breach is the same, please consolidate the appropriate information into one row of the table and state how many breaches the related information applies to.

The table was largely consistent with the table for provision of credit breaches.

10.2. How many applications for credit were approved and finalised/settled by the bank during 2016–17 which are secured by a guarantee?

10.3. What percentage of credit accounts held by the bank are secured by a guarantee as at 30 June 2017?

10.4. The CCMC is seeking information about the type and amount of monitoring conducted by the bank to support compliance with the guarantees Code obligations between 1 July 2016 and 30 June 2017. Please use the questions below as a guide to providing this information. If the specific wording does not reflect the terms used by the bank or its approach to Code monitoring, please provide any additional or different information along with an appropriate explanatory note.

10.4.1. Please provide a summary of the monitoring methods that were in place between 1 July 2016 and 30 June 2017, including:

- a description of the actions
- who/what performs the actions (role(s)/type of system)
- how the actions are performed
- how regularly the action is performed, and
- why the action is performed

for each type of monitoring activity.

10.4.2. Please provide details about the amount of monitoring undertaken by the bank relating to guarantees between 1 July 2016 and 30 June 2017, for example:

- Any quality assurance reviews conducted.
- Any reporting and monitoring conducted on the bank's processes/procedures or IT systems associated with guarantees.

- Whether any additional, exceptional or targeted monitoring or reviews were conducted.
- Any monitoring conducted by the bank's third line of defence or internal audit function.

11. Feedback on the provision of Code compliance information to the CCMC

The CCMC wishes to understand the challenges faced by the bank when providing qualitative and quantitative information to the CCMC.

11.1. Please describe the challenges faced by the bank when completing this CCMC questionnaire, including but not limited to:

- providing the requested information in the breach details tables, and
- providing information about levels of monitoring undertaken overall or in relation to specific Code obligations.

11.2. Please describe the challenges faced by the bank, and/or the steps the bank needs to take, to provide quantitative information to the CCMC for own motion inquiries and annual compliance statements. For example, data regarding:

- credit applications
- levels of monitoring undertaken
- requests for financial difficulty assistance
- complaints
- small business customers.

11.3. How can the CCMC improve its current data collection regarding:

- the types of information requested, and
- the method and frequency of collecting that information?

11.4. What additional information, not currently collected by the CCMC, does the bank consider would assist the CCMC in its aim to provide assurance to the community that the Code is being actively monitored?

11.5. Please provide any other feedback the bank would like to make about the CCMC's monitoring and data collection methods.

END OF REPORT