BCCC Guidance Note No. 1

Breach Identification and Reporting

This Guidance Note sets out the Banking Code Compliance Committee's expectations for how Code subscribing banks should identify, record and report breaches of the 2019 Banking Code of Practice.

About the BCCC

The Banking Code Compliance Committee (BCCC) is an independent compliance monitoring body established under clause 207 of the 2019 Banking Code of Practice (Code).

The purpose of the BCCC is to monitor and drive best practice Code compliance. To do this the BCCC will:

a. examine banks practices
b. identify current and emerging industry wide problems
c. recommend improvements to banks' practices
d. consult with and keep stakeholders and the public informed.

Guidance Notes

Guidance Notes are subject to change by the BCCC and this document reflects the BCCC's views as at the date of publication. The BCCC considers all matters on the basis of their individual circumstances and this document does not anticipate all possible issues that might come before the BCCC.

Publication date: 13 September 2019

Introduction

1. This Guidance Note sets out the Banking Code Compliance Committee's (BCCC) expectations for how Code subscribing banks (banks) should identify, record and report breaches of the 2019 Banking Code of Practice (the Code).

2. Comprehensive breach data reporting is essential for banks to demonstrate accountability for their compliance with the Code. The BCCC expects banks to have methodical processes in place to ensure that breaches are identified and corrected, and to be transparent in their reporting to the BCCC.

3. The BCCC requires banks to report high quality breach data in a form that is consistent across the industry.

The BCCC's compliance monitoring program

4. The BCCC's compliance monitoring program comprises of three types of activities:

    a) investigations
    b) inquiries, and
    c) data collection.

5. The BCCC has published a separate Operational Procedure that explains how it will make breach findings as a result of its investigations and inquiries (*Operational Procedure: Making a finding of non-compliance*).

6. This Guidance Note is focused on the BCCC's expectations of banks to self-identify and report Code breaches.

BCCC data collection

7. The BCCC can request breach data to monitor and assess banks compliance with the Code (BCCC Charter clause 4.2). The BCCC has created the Banking Code Compliance Statement (Compliance Statement) to collect breach data.

8. Banks are required to report breach data two times per year. The Compliance Statement will be in a consistent form that is approved by the BCCC every two years, following consultation with banks.

Code monitoring and breach identification

9. The Code sets out banks' commitments and promises to their customers and the wider community. The BCCC expects banks to have a comprehensive and well-documented framework for monitoring compliance with the promises made in the Code.

10. The BCCC requires banks to consider all Code obligations when conducting any compliance assessments and not just those that are aligned to existing legislation or regulation.

11. Banks monitoring programs should include a broad range of methods to identify incidents that may be breaches of the Code, including for example:

    a) quality assurance reviews, such as call monitoring
    b) system monitoring
    c) reviews of customer complaints and feedback
    d) performance audits, and
    e) controls testing.

12. Under clause 9 of the Code, banks are required to train staff to understand and comply with the Code. The BCCC expects that as a result, staff will be able to recognise situations and incidents where the Code may not have been complied with. Banks should create a positive compliance culture by encouraging staff to report any such incidents to relevant leaders and risk and compliance teams. Banks should develop simple processes to support this type of reporting.

13. Banks should have a mechanism for collating the details of all identified incidents that may include a breach of the Code.

Breach assessment and remediation

14. Chapter 3 of the Code, '*Our compliance with the Code'*, states that banks will honour the commitments made in the Code. A breach of the Code is when a bank does not honour those commitments, or more plainly, the bank fails to comply with a Code obligation.[1]

15. Appropriately skilled staff within the bank should assess all incidents to determine whether there has been one or more breaches of the Code arising from the bank's conduct.

16. More than one Code obligation will often apply when a bank interacts with a customer. For example, when a customer is applying for a loan, requesting financial difficulty assistance or making a complaint, the following obligations will apply:

    a) engage in a fair, reasonable and ethical manner (clause 10)
    b) train staff and representatives to competently do their work (clause 9)
    c) communicate in a timely manner and provide information that is useful and clear (clause 17)
    d) answer questions about banking services (clause 22)
    e) train staff to treat diverse and vulnerable customers with sensitivity, respect and compassion (clause 33)
    f) enhance access to banking services for people with a disability and older customers (clause 34), and
    g) take extra care when providing banking services to vulnerable customers (clauses 38 to 41).

17. The bank's assessment of incidents should consider all Code obligations and the relationship between different Code obligations. All Code breaches identified as a result of the assessment should be recorded and not just the most obvious or relevant breach.

[1] A breach of any Code obligation will also be a breach of Chapter 3, clause 8. Banks are not required to record or report breaches of clause 8.

18. For the purposes of recording Code breaches, incidents should be assessed as follows:

    a) Where an incident results in multiple breaches of the same type, this is to be counted as one breach of the relevant Code chapter or obligation. For example, a systems error that results in multiple customers not receiving deposit account statements, should be recorded as one breach of Chapter 31. This example would be considered a systemic Code breach because the breaches share the same root cause (see paragraph 38).

    b) Where an incident results in more than one breach of the Code's obligations that are not of the same type, each breach should be recorded. For example, where a staff member does not work with a customer to help them find a solution to their financial difficulties, this may include one or more breaches of both Chapter 41 (financial difficulty) and Chapter 4 (staff training and engaging in a fair and reasonable manner).

19. The BCCC expects banks to record every Code breach regardless of the level of significance or materiality of the breach.

20. For each breach that is identified, the bank should take all appropriate steps to stop the breach recurring and to remediate customers affected by the breach. These actions must also be recorded by the bank.

Breach reporting

Banking Code Compliance Statement

21. The BCCC recognises that banks may report legislative or regulatory breaches to regulators based on an assessment of a breach's significance or materiality. The Code and BCCC Charter make no reference to such a requirement and as previously stated, the BCCC requires banks to record all Code breaches. The BCCC may make a Finding of whether a breach is systemic or serious, where it considers it necessary, by following the *BCCC Operating Procedure: Making a finding of non-compliance.*

22. Banks are required to report all Code breaches to the BCCC in the Compliance Statement submitted following the relevant period. Banks will do this by listing the total number of breaches identified under each chapter of the Code.

23. Banks are required to provide further details of incidents or events that include Code breaches that meet one or more of the following criteria:

    a) the bank or any external body (for example, the Australian Securities and Investments Commission (ASIC), the Australian Financial Complaints Authority (AFCA) or the BCCC) has considered the breach of the Code to be 'significant', 'systemic' or 'serious'[2]

[2] By any classification used by the bank or the external body. The Charter states that 'external body' includes but is not limited to, any court, tribunal, arbitrator, mediator, independent conciliation body, dispute resolution body, complaint resolution scheme (including, for the avoidance of doubt, AFCA), statutory Ombudsman, or agency and agency appointed review in any jurisdiction. The BCCC also considers ASIC to be a relevant external body.

b) the incident affected more than one customer, or
c) the incident had a financial impact of more than $1,000 on a customer or the bank.

24. In addition, the bank is required to report the details of a random sample of 5% of the total number of breaches for each Code chapter (or at least 1 breach if the total for a chapter is less than 20 breaches) that do not meet any of the criteria listed in paragraph 23 above. [3]

25. The details of an incident that the bank is required to provide include:

a) a description of the incident
b) the type of product or service associated with the incident
c) the business unit within the bank where the incident occurred
d) the cause(s) of the incident
e) how the incident was identified
f) remediation provided to customers
g) actions taken to prevent recurrence
h) the number of customers impacted
i) the type of 'customer' impacted (for example, individual, small business, guarantor)
j) the total financial impact on the customer(s) or the bank
k) the relevant Code chapters that have been breached, and
l) the number of breaches of the relevant Code chapters.

Other breach notifications

26. The BCCC considers it good practice for banks to keep it informed of material non-compliance with the Code in a timely manner.

27. For that reason, the BCCC requests that banks report to it any non-compliance with the Code that:

a) is a breach of financial services laws, and
b) has been reported to ASIC.

28. The BCCC requests that this information be provided to the BCCC within 21 business days of the date the matter was reported to ASIC.

BCCC response to breach reporting

Reporting

29. The BCCC analyses the information provided by banks and reports on the outcomes both publicly at an aggregated industry level and individually to each bank.

30. In accordance with clause 4.2 of the BCCC Charter, reports will allow banks to assess their Code compliance relative to other banks.

[3] The bank is required to provide a summary of how it generated the sample.

The BCCC's Code Monitoring Priority Framework

31. The BCCC conducts its compliance monitoring program with reference to its Code Monitoring Priority Framework (see the BCCC's *Operational Procedures* for further information).

32. The breach data collected from banks is used by the BCCC to inform its future monitoring priorities.

33. In some cases, the BCCC may consider it appropriate to initiate a 'targeted inquiry' (see *Operational Procedures*) into a breach or incident reported to it by a bank.

Classification of breaches

Breaches

34. For the purposes of reporting to the BCCC, banks are required to assess whether an incident does or does not include a Code breach.

35. A breach of the Code occurs when a bank fails to comply with a Code obligation.

Systemic and serious breach findings

36. When concluding a major inquiry, targeted inquiry or a compliance investigation, the BCCC may make a Finding as to whether it considers a bank has breached the Code and whether a breach is systemic or serious.

37. The BCCC may also impose one or more sanctions after considering the seriousness of a breach.

Systemic breaches

38. A systemic breach is a breach:

    a) that has affected, or is likely to affect, more than one party, and /or
    b) where multiple breaches share the same cause. [4]

Serious breaches

39. The BCCC will consider the following factors when considering whether a breach constitutes a serious breach and whether to impose a sanction:

The bank's actions that led to the breach

    a) The extent to which it considers that the bank's actions were:

        i. wilful
        ii. negligent

[4] 'Party' has the same meaning as "you" and "your" in Chapter 1 of the Code.

iii. diligent or prudent, and/or
iv. fair, reasonable and ethical.

b) The extent to which the breach indicates that the bank's framework to ensure compliance with Code obligations is inadequate.

The impact of the breach/materiality

c) The amount of harm caused or likely to be caused by the bank's actions.
d) The nature, scale and complexity of the banking product or service.

The bank's actions to address the breach

e) Whether the bank's actions to remediate the customer are sufficient and appropriate.
f) The steps taken to remedy the conduct or errors that led to the breach.
g) The sufficiency of the bank's steps to prevent or minimise recurrence.
h) The steps taken to act on a BCCC Finding or undertaking related to a previously self-reported breach.

The bank's engagement with the BCCC

i) The bank's historical record of compliance with the Code, including the number or frequency of similar previous breaches.
j) The bank's history of engagement and cooperation with the BCCC or its predecessor entities.
k) Whether the bank has, without reasonable excuse, failed to respond to or comply with a reasonable BCCC request.