CODE COMPLIANCE MONITORING COMMITTEE
(the CCMC)

Guidance Note No. 12

Classification, Reporting and Remediation of Non-Compliance with the Code of Banking Practice

The CCMC is an independent code compliance monitoring body established under clause 36 of the Code of Banking Practice (the Code).

The CCMC oversees the compliance of subscribing banks with their code obligations by:

a. monitoring compliance with the Code
b. investigating code breach allegations, and
c. monitoring any aspects of the Code that are referred by the Australian Bankers Association (the ABA).

This Guidance Note has three purposes, namely to indicate the CCMC's likely approach to:

a. the classification, recording and reporting of non-compliance with the Code in the discharge of its functions
b. its enforcement and sanctions powers and how they apply to different levels of non-compliance, including
c. the public naming of a code subscriber.

Guidance Notes are subject to change by the CCMC and this document reflects the CCMC's views as at the date of its publication.

It is important to understand that the CCMC considers all matters on the basis of their individual circumstances and this document is not intended to anticipate all possible issues that might come before the CCMC.

Any reference to "bank" in this Guidance Note means a bank which subscribes to the Code. Any reference to the "Code" is a reference to the 2013 version of the Code, unless otherwise stated. Any reference to a "consumer" or "customer" means an individual or small business that is either a customer or potential customer of a bank.

When considering whether a bank has complied with the provisions of the Code, the CCMC will also have regard to the key commitments made by that bank to act fairly, reasonably and ethically in the provision of services to its customers and to comply with all relevant laws.

For more information about the CCMC, please visit its website: www.ccmc.org.au.

Introduction

1. The CCMC's Mandate[1] sets out its powers and functions which are interpreted in conjunction with clause 36 of the Code.

2. One of the CCMC's functions is to monitor the compliance of banks with the Code. This is done using a number of methods, including lodgement of an Annual Compliance Statement (ACS) by banks that reports on their compliance with the Code during the previous 12 months.

3. Independent monitoring by the CCMC is important to ensure that non-compliance with the Code is identified, reported and remedied. Robust compliance monitoring arrangements are essential to maintain public confidence that banks comply with, and are seen to comply with, the Code's obligations.

4. The CCMC is also responsible for the investigation and determination of whether a breach of the Code has occurred.

5. The CCMC must report annually on the outcomes of its activities and functions including the level of compliance with the Code, the underlying cause of non-compliance, any compliance measures implemented by relevant banks and any systemic breaches or other trends.

6. The CCMC has a range of actions for enforcing code obligations. This includes the naming of a bank on the CCMC's website, in its Annual Report, or both, in connection with a breach of the Code where a bank has been guilty of serious or systemic non-compliance.

7. To facilitate the effective, efficient and transparent discharge of all of these functions, this Guidance Note outlines the CCMC's likely approach to the classification, recording and reporting of non-compliance (breaches) with the Code's obligations and the subsequent approach that the CCMC may take to ensure remediation of non-compliant activity or sanction against the relevant bank.

Classification of code breach activity

8. When undertaking its functions to monitor or investigate compliance with the Code, the CCMC may become aware of breach activity or make a Determination that a bank has not complied with its code obligations.

9. Non-compliance with the Code is classified by the CCMC, as follows:

    9.1. a breach (non-compliance with a code obligation)
    9.2. a significant breach
    9.3. a serious breach, or
    9.4. a systemic breach of the Code.

10. Appendix 1 outlines these classifications in more detail and the CCMC's likely approach when enforcing the Code against banks.

[1] The CCMC's Mandate can be found at http://www.ccmc.org.au/the-code/

11. The classifications are not mutually exclusive. Some overlap in classification may occur. For example, a significant breach of the Code may have resulted from systemic non-compliance with code obligations.

12. When making a decision about non-compliance with the Code, the CCMC will consider whether a breach is significant and/or serious or systemic in nature. A significant breach is not necessarily serious or systemic and a systemic breach is not necessarily significant.

Breaches

13. A breach of the Code is described as a failure to comply with the obligations of the Code in the provision of a banking service.

14. The CCMC expects that banks will undertake any remediation that is appropriate to correct non-compliance.

Significant breaches

15. When assessing the significance of a code breach, the CCMC will be guided by Australian Securities and Investments Commission (ASIC) "Regulatory Guide 78 – Breach Reporting by AFS Licensees", the Australian Standard "AS 3806 2006 - Compliance Programs" and Section 912D of the Corporations Act 2001 (Cth).

16. A significant breach of the Code's obligations therefore will be determined on a case-by-case basis, by reference to matters such as the:

    16.1. number of customers affected or likely to be affected
    16.2. extent of any customer detriment
    16.3. adequacy of arrangements to ensure compliance with the Code
    16.4. duration of the breach
    16.5. number and duration of similar breaches
    16.6. rectification and other costs incurred or to be incurred
    16.7. impact of the breach on the bank's ability to provide services, and
    16.8. extent to which the breach indicates the bank's arrangements for compliance with the Code are inadequate.

17. To assist banks in their code breach assessment processes, some examples of significant breaches that have been reported to the CCMC in the past include:

    17.1. incorrect disclosures in a Product Disclosure Statement
    17.2. inaccurate advertising of product and interest rate details
    17.3. procedures that do not comply with another code, for example Debt Collection or Centrelink Guidelines
    17.4. multiple errors affecting a class or classes of customers, for example charging of incorrect interest rates or failure to act on direct debits cancellation instructions
    17.5. multiple minor instances of failure to comply with code obligations affecting a class or classes of customers, for example customers in financial difficulties, and
    17.6. failure to follow the guarantee provisions resulting in significant customer detriment.

18. When the CCMC becomes aware of, or identifies a significant breach of the Code, it may:

18.1. seek further information from the bank about how the issue has or will be remedied to prevent recurrence, and/or
18.2. engage in a monitoring program to ensure that actual or proposed remedial action has been completed.

19. The CCMC will publish details of any significant breaches of the Code in its Annual Report and on its website. These publications will be on a de-identified basis, unless the CCMC has decided to publically name a bank (see paragraphs 57–70).

Serious breaches

20. A breach of the Code that is classified by the CCMC as non-compliance which is fraudulent, grossly negligent or involves willful breaches of the bank's code obligations will be considered to be serious. It may also include instances where a bank has not taken steps to remedy the conduct or errors that led to the breach, or willfully ignores or fails to act on a CCMC Determination or undertaking[2] related to a previously self-reported significant and/or systemic breach.

21. This description is consistent with the definition of *serious misconduct* used in the Terms of Reference of the Financial Ombudsman Service Australia (FOS).

22. A serious breach of the Code is considered by the CCMC to be the highest threshold of breach and will always be significant in nature.

23. The CCMC may conclude a compliance investigation by Determination. In doing so the CCMC must first issue a Notice of Determination in accordance with Mandate clause 10.3(a)(ii) that includes, if applicable, a brief description of any finding the CCMC intends to make that the bank is responsible for serious or systemic non-compliance with the Code.

24. Where a breach is classified as serious, the CCMC is likely to increase its level of engagement with the bank to understand what occurred and why, and how the bank plans to respond to and rectify the non-compliance.

25. In accordance with clause 36(j) of the Code and clause 11 of the CCMC Mandate, the CCMC may consider the public naming of a bank where the bank has been, amongst other things, guilty of serious or systemic non-compliance.

Systemic breaches

26. Non-compliance with the Code that has implications beyond the immediate actions and parties affected will be considered to be systemic. This is consistent with the definition of *systemic issue* in the FOS Terms of Reference.

27. Systemic breaches are those which have, or are likely to affect, more than one person. It may also involve a process, policy or technological issue affecting the the bank's operations.

28. The CCMC believes that systemic non-compliance is likely to be a lower threshold than a serious breach of the Code. The same conduct may or may not constitute a significant breach of the Code, using the criteria set out in paragraph 16 above.

[2] In the absence of a formal definition in the Code or Mandate, the term "undertaking" is given its ordinary meaning by the CCMC and means a formal pledge or promise to do (or not do) something.

29. To determine whether a code breach is systemic, the CCMC may request access from a bank to complaints data, product details and internal processes and procedures documentation.

30. Banks should self-report systemic breaches of the Code to the CCMC. If they do so, they should provide details of what occurred, the impact of the breach including the number of consumers affected and detriment caused and the remedial action that has been, or will be, taken to correct the non-compliance and prevent recurrence.

31. Where the CCMC makes a Determination that a code breach is systemic, in addition to recording a code breach against the bank, the CCMC may request additional information about the remediation program the bank will or has undertaken to correct the non-compliance and prevent recurrence and monitor the completion of that program.

32. The CCMC reports on systemic breaches in its Annual Report. This will be on a de-identified basis, unless the CCMC has decided to publically name a bank (see paragraphs 57–70).

33. The CCMC may initiate an Own Motion Inquiry into the issues associated with a systemic breach across all banks, where it believes there may be a risk of broader industry non-compliance.

Arrangements for recording and reporting code breaches

34. The CCMC expects banks to:

    34.1. have a clear and well understood process for identifying, recording, reporting and rectifying non-compliance with the Code
    34.2. ensure that arrangements are in place to prevent a recurrence of breach activity, and
    34.3. have appropriately trained personnel within each operational area to identify and report when and where breaches have occurred.

35. Breach incidents may typically arise across all of the bank's operational areas and systems in addition to direct dealings with customers (including branches, collections activities and call centres).

36. When recording breach activity, multiple breaches of the Code may be recorded as follows:

    36.1. a single incident that results in breaches of the same type (for example a system error that resulted in breaches of the Code's disclosure provisions and has impacted a number of customers) may be counted as one breach or a significant breach of the relevant Code clause, and

    36.2. where more than one of the Code's standards has been breached (for example a customer's bank account details are disclosed to a third party and their complaint about this is not dealt with in accordance with internal dispute resolution time frames) both breaches of the Code should be recorded.

37. In accordance with clause 36(b)(iii) of the Code, once a bank has identified non-compliant conduct with the Code's standards, it should assess whether that breach has resulted in a failure to act fairly and reasonably in a consistent and ethical manner in the

provision of services to its customers (clause 3.2) and/or to comply with all relevant laws relating to banking services (clause 4.1).

When must code breaches be reported to the CCMC

38. Clause 36(f) of the Code requires each bank to lodge (in a form acceptable to the CCMC) an Annual Compliance Statement (ACS) with the CCMC on its compliance with the Code during the previous reporting year. This Statement forms a key part of the CCMC's program to monitor banks' compliance with the Code.

39. The number of breaches of the Code to be reported should include information from all sources (including the bank, the CCMC, FOS and other forums) and be recorded against the relevant clause of the Code.

40. Banks are required to report significant breaches separately in the ACS.

41. The CCMC accepts that banks have systems and procedures to identify and report significant breaches of their legal obligations. The recording and reporting of significant code breaches to the CCMC therefore may be made according to the criteria the bank already applies to determine breach significance (or similar terminology) for its own reporting, both internally and to other regulators (see paragraphs 15 -19 of this Guidance Note).

42. When completing the significant breach table within the ACS, the following information should be provided:

Incident Details	The version of the Code which applies; clause breached; date detected; product category; channel; customer type; location; role/ position of identifier; nature/characteristics; and manner discovered.
Underlying Causes	Matters involved; system/process issues; and personnel issues.
Breach Magnitude	Systemic significance; number of customers affected (actual/ potential/ direct/ indirect); location of customers affected (actual/ potential/ direct/ indirect); duration/ dates over which breach occurred; payments to customers; other rectification costs incurred; and non-financial impacts.
Remedial action	Actions with dates; preventative/ corrective; short/ long-term; temporary/ permanent; and past/ present/ future.

43. Where a breach of the law has been reported to, or identified by, ASIC or another regulator and the incident has also resulted in a breach of the Code, this breach should be reported to the CCMC when reported or identified or in the Code Breach Summary in the ACS.

44. This is the same for breaches of the Code that are determined by another forum, namely any court, tribunal, arbitrator, mediator, FOS, or statutory ombudsman in any jurisdiction.

45. The CCMC may also invite a bank during a reporting year to acknowledge that a breach of the Code has been found by another forum or regulator and/or indicate to the CCMC whether the breach will be self-reported in the ACS.

46. If a bank self-reports an individual breach outside the ACS program, the CCMC will acknowledge the report and may request further information if needed.

47. In some cases the CCMC may not need to take any further action if the reported breach has been rectified to the CCMC's satisfaction.

48. The CCMC may also contact the bank to discuss improvements made or proposed to code compliance processes and procedures to prevent recurrence, if it is not satisfied that this has occurred.

49. A failure by a bank to report breaches of the Code to the CCMC may of itself, in certain circumstances, be a breach of clause 36(f) of the Code.

50. The CCMC acknowledges that banks may wish to annually self-report unique breaches of clauses 3 and 4 separately to the CCMC, without linking to a corresponding breach of the Code's standards. Provision is made for this type of annual reporting in the ACS.

Publication of code breach activity

51. The effective notification by banks of code related breaches allows the CCMC to report on and make recommendations regarding emerging areas of risk and the continuous improvement of industry standards.

52. The CCMC will also add this data to internal risk models for ongoing monitoring of trends in code compliance.

Possible enforcement action

53. Appendix 1 to this Guidance Note outlines some of the potential actions available to the CCMC in its dealings with the banks to address and resolve non-compliance with the Code.

54. These actions may be broadly categorised as:

    54.1. Guidance on good industry practice
    54.2. Negotiation and resolution
    54.3. Remediation and Corrective actions
    54.4. Determination
    54.5. Undertakings
    54.6. Warnings, and
    54.7. Public naming

55. These actions are not mutually exclusive and may be used in combination.

56. The level of engagement a bank can expect from the CCMC and the application of the CCMC's enforcement and sanctions powers once code breach activity has been identified, will be commensurate with the level of non-compliance the CCMC considers the bank has engaged in.

Public naming of a bank

57. The CCMC is accountable to its stakeholder groups for the transparency of its code monitoring and enforcement actions.

58. Transparency, through public disclosure of sanctions imposed in certain circumstances, is considered by the CCMC to be an important factor to ensure that the banks are held, and are seen to be held, accountable for their compliance with code obligations. ASIC

Regulatory Guide 183[3] for example, points out that community confidence in the effectiveness of industry codes is largely reliant on the perception that a code is seen to be enforced against non-compliant subscribers.

59. The most serious sanction that the CCMC may impose is the public naming of a bank.

60. Clause 36(j) of the Code states that the CCMC may name a bank on the CCMC's website, in the next CCMC Annual Report, or both, in connection with a breach of the Code where it can be shown that the bank has:

    60.1. been guilty of serious or systemic non-compliance
    60.2. ignored the CCMC's request to remedy a breach or failed to do so within a reasonable time
    60.3. breached an undertaking given to the CCMC, or
    60.4. not taken steps to prevent a breach reoccurring after having been warned that the bank might be named.

61. Clause 11 of the Mandate reiterates that the CCMC may name a bank in accordance with clause 36(j) of the Code.

62. The CCMC recognises that the objective in imposing a public naming sanction can be different in each case. For example, a naming power may be used to reprimand a bank that has failed to comply with a request by the CCMC to correct a breach of the Code and/ or to act as a general deterrent to others to avoid engaging in non-compliant conduct.

63. The CCMC accepts that the publication of a bank's name for non-compliance with code oblgiations may have significant consequences.

64. In considering whether or not to publically name a bank in a particular matter, the CCMC will balance the public interest in publishing the non-compliant activity against the rights of the bank that is to be the subject of the sanction.

65. The CCMC may also take into account a number of factors when deciding whether to publish or not, including:

    65.1. any limitations outlined in the Mandate or the Code
    65.2. the need to safeguard confidential or sensitive information, pursuant to clause 14 of the Mandate
    65.3. privacy legislation and guidelines
    65.4. the need to apply procedural fairness and consider fairness in all the circumstances
    65.5. the risk of harm or detriment that may be caused to any of the parties, and
    65.6. compliance with any court orders not to disclose information in certain circumstances.

66. In applying these criteria, the CCMC will consider the public naming power in the context of what is reasonable in all of the circumstances of each case, having regard to legal principles relevant to the decision-making process, applicable code provisions and any CCMC guidance as to code requirements.

[3] Australian Securities and Investments Commission, 2013, *Regulatory Guide 183: Approval of financial services sector codes of conduct*, p. 9

67. If the CCMC forms the view that it should consider imposing a public naming sanction, the CCMC will:

    67.1. notify the bank and the bank's CEO of the proposal, prior to a final decision being made
    67.2. provide a brief description of the finding the CCMC intends to make and the reasons for why it reasonably suspects that the bank is responsible for serious or systemic non-compliance with the Code or any other breach of clause 36(j) of the Code
    67.3. advise the bank of the opportunity to be heard on the proposed sanction and make submissions within 28 days of the date of the notice as to why the sanction should not be imposed, and
    67.4. include a statement that the proposed sanction will become effective after 28 days from the date of the notice should no submissions be received.

68. At the expiry of the 28 day notice period:

    68.1. if the bank has not responded, the sanction will be adopted, or
    68.2. if the bank has responded, the CCMC will consider the submissions made, prior to making its final decision.

69. The CCMC may also consult with the FOS Chief Ombudsman and Australian Bankers' Association (the ABA), as parties to the Code's governance arrangements, about its proposal to impose a naming sanction against a particular bank prior to publication occuring.

70. Once the CCMC decides that a public naming sanction is to be imposed the CCMC will notify the CEO of the bank of its decision and:

    70.1. prepare a publication notice which includes:

        70.1.1. the name of the bank
        70.1.2. the date of the CCMC's decision
        70.1.3. the Code obligations that have been breached
        70.1.4. the relevant subsection of clause 36(j) to which the CCMC's decision relates, and
        70.1.5. a short statement of the CCMC's reasons for the decision

    70.2. provide a copy of the notice to the bank and the ABA
    70.3. provide a copy of the notice to the FOS Chief Ombudsman, and
    70.4. include the notice in the CCMC's next Annual Report and/or on its website.

Appendix 1

CCMC's classifications of non-compliance

A **serious breach** is non-compliance with the Code which is considered to be fraudulent, grossly negligent or wilful. It may also include instances where a bank has not remedied the conduct or errors which led to the breach, or willfully ignores or fails to act on a CCMC Determination or undertaking related to a previously self-reported significant and/or systemic breach.

A serious breach is the highest threshold of breach (and will always be significant).

A **significant breach** is a breach of the Code's obligations that is determined to be significant on a case-by-case basis, by reference to matters such as the:

- number of customers affected or likely to be affected
- extent of any customer detriment
- adequacy of arrangements to ensure compliance with the Code
- duration of the breach
- number and duration of similar breaches
- rectification and other costs incurred or to be undertaken
- impact of the breach on the bank's ability to provide services, and
- extent to which the breach indicates the bank's arrangements for compliance with the Code are inadequate.

Consideration given to ASIC "Regulatory Guide 78 – Breach Reporting by AFS Licensees", the Australian Standard "AS 3806 2006 - Compliance Programs" and Section 912D of the Corporations Act 2001.

Code subscribing banks are required to report significant breaches separately in the Annual Compliance Statement.

The CCMC will give consideration to the criteria above when making a Determination on whether there is a breach of the Code.

A **systemic breach** is non-compliance that has implications beyond the immediate actions and parties affected by the non-compliance with the Code.

Systemic breaches are those which have or are likely to affect more than one person. It is likely to involve a process, policy or technological issue within the bank's operations.

A systemic breach is likely to be a lower threshold than a serious breach, and may, or may not, be significant.

A **breach** is a failure to comply with the obligations of the Code in relation to the provision of a banking service.

The CCMC may become aware of breaches or make a Determination that a bank has not complied with the Code, as a result of:

- a bank self reporting breaches in the Annual Compliance Statement
- an investigation into an allegation that a bank has breached the Code
- an investigation into a referral from the Australian Bankers' Association (ABA)
- another forum hearing an allegation and that forum making a determination that a bank has not complied with the Code, or
- through another monitoring process such as an Own Motion Inquiry (which may lead to a CCMC investigation or self-reported non-compliance).

CCMC's likely action in enforcing code obligations