CUSTOMER OWNED BANKING CODE COMPLIANCE COMMITTEE

Completing the 2023 Customer Owned Banking Annual Compliance Statement (ACS)

Your ACS is due on or before ***30 September 2023***.

Before you begin

- Review your internal policy and procedures relating to Code compliance.
- Assess and verify your staff awareness of Code obligations.
- Review your staff training to include compliance with Code obligations.
- Review your Code compliance reporting and monitoring process.
- Assess and verify your Code compliance data.
- Review your internal complaints reporting and monitoring process.
- Assess and verify your internal complaints data.

When completing the ACS

- Record data for the reporting period ***1 July 2022 to 30 June 2023***.
- Provide enough information to address each item in full.
- Highlight any changes to frameworks, processes or procedures in the reporting period.
- Ensure that the data you provide is accurate and complete.
- Ensure that the data does not include any information that is personal, private or can identify people or institutions.
- Upload any necessary supporting documents.

After you submit

- Download a copy of your final submission for your own records.
- We may contact you if we need more information to assess your compliance with the Code.

Further assistance

- Daniela Kirchlinde, Senior Manager - Code Compliance and Operations dkirchlinde@codecompliance.org.au
- Tania Meadows, Senior Compliance Analyst tania.meadows@codecompliance.org.au

Background

The Customer Owned Banking Code of Practice

2018 Code

The Customer Owned Banking Code of Practice became effective 1 July 2016 and was updated in 2018 to accommodate changes that the Australian Securities and Investments Commission (ASIC) made to the Regulatory Guide 221 *Facilitating digital financial services disclosures* and the *e-Payments Code*.

2022 Code

The Code was updated again in 2022 and came into effect on 31 October 2022.

Transition period

The 2023 ACS requests Code subscribers to self-report breach and complaints data under both Codes:

- the 2022 Code applies to the period 31 October 2022 to 30 June 2023
- the 2018 Code applies to the period 1 July 2022 to 30 October 2022.

This document uses a thematic approach to help Code subscribers transition to the 2022 Code by providing references to both the 2018 Code and the 2022 Code.

Code subscribers can choose to refer to the 2022 Code for the entire period.

Purpose of the ACS

The ACS program is a central component of our monitoring work.

It asks for information about your Code compliance frameworks, including breach and complaints reporting and monitoring, as well as your institution's overall compliance culture.

The ACS helps us to:

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

Data collected through the ACS program will be aggregated, de-identified, analysed for trends and patterns and published in our Annual Data Report. We will also provide data to Code subscribers via individualised Benchmark Reports.

See previous publications on our website.

Changes to the ACS

There were minor changes to the 2023 ACS:

Table 1: Changes to the 2023 ACS

Section	*Description of the change*	*Reason for the change*
C.1 Detailed Breach reporting	Improved detailed breach reporting via the Breach Data Detail Report including: • reordering of Code references (2022 Code is the first selection) • product/service type and description • root cause • immediate remedial action • timeframe for immediate remedial action • long term remedial action • timeframe for long term remedial action, and • reported to regulator. Information about options listed in the drop-down menu are provided in *Table 2* and *Table 3*.	Following feedback from the 2022 ACS, we updated the Breach Data Detail Report to include additional options that fit an organisation's needs. We encourage Code subscribers to self-report under the specific Code obligations (Part D of the 2018 Code and Part B of the 2022 Code), not the Key Promises. Doing so provides more meaningful information and data to identify specific areas of concern.
C.2 No long-term remediation actions	Request to provide detailed information about the processes you have to review a breach incident and take action to prevent future breaches. This contrasts with immediate remediation action which aims to limit the impact of a breach.	We noted the lack of detailed information about long-term remediation actions. It often was the same as the immediate remediation action.
D.3 Products	Inclusion of product categories regarding: • General Insurance (as per ASIC reference 40 to 70) • Small business/farm insurance (as per ASIC reference 65 to 79) • Life Insurance (as per ASIC reference 114 to 125) • Superannuation (as per ASIC reference 143 to 178) For detailed information and categories, see ASIC IDR Data Reporting Handbook.	This comes following feedback and recommendations from Code subscribers who provide these products and services.
D.5 Outcomes	Deletion of category 'unresolved/open as at 30 June'.	Deemed to be irrelevant for respective analysis.

Section A: Declaration

This part of the ACS requests information that will help us understand the size of your organisation.

Certification Details

The information provided in the ACS must be certified by the Chief Executive Officer (CEO) or Chief Risk Officer (CRO) of your organisation.

The ACS is an opportunity for Code subscribers to review their data for the reporting period and reflect on any learnings to share with the COBCCC.

Size of your organisation

Confirm:

- assets in dollars
- number of members
- number of open accounts
- full-time equivalent staff.

We use this information to benchmark data collected from all Code subscribers.

Number of branches

Report the number of branches your organisation has across the country.

A branch is considered an office of your organisation and any authorised representative.

Section B and C: Code Breach reporting

This section of the ACS deals with instances of Code non-compliance. It asks you to record the number of breaches of each Code section in a table, including specific details of each breach in the ***COB Breach Data Detail Report 2023***.

Definition of Breach

A failure to comply with the obligations of the Code in relation to the provision of a customer owned banking service.

Reporting of breaches

Report all breaches regardless of remediation activities.

Sourcing breach data

Code subscribers typically source breach data from consolidated compliance registers. If these do not cover all Code breaches, review other sources, such as complaints records for breach incidents, file audit and external audits.

Breaches can arise in all operational areas, in direct dealings with customers (such as in branches, collections and call centres), and in other areas such as marketing. Identifying Code breaches should include oversight of all such areas by appropriately trained personnel.

Classification of breaches under specific obligations

Categorise breaches against the primary reason for non-compliance. Classify instances of non-compliance against specific Code obligations. Avoid listing breaches under general obligations (such as 'Key Promises').

Most Code breaches should fall under specific Code obligations (Part D of the 2018 Code and Part B of the 2022 Code), **not** the Key Promises.

Example

For examples and classification of Code breaches, please refer to the COBCCC Annual Data Reports.

Detailed information for each Code breach

Please use the ***COB Breach Data Detail Report 2023*** to specify details for each Code breach. Download this spreadsheet via the online portal. We previously emailed a sample to you.

Recording incidents that involve multiple breaches

We want to avoid duplication in reporting Code breaches.

When the nature, cause and outcome of more than one breach is the same, consolidate the information into one row of the table and state how many breaches it applies to.

To compile breach reporting totals, use the following:

- For a single incident that results in breaches of the same type, count it as a single breach of the relevant Code section.

  ***Example**: A system error causes a specific mistake to happen 60 times. This is a single breach with the commentary section noting that it occurred 60 times (e.g., 60 customers were affected).*

- For a single incident that results in breaches of more than one Code section, record the breach only against the primary Code section.

  ***Example:** A customer's privacy is breached, and their complaint is not dealt with in accordance with internal dispute resolution timeframes. Record the main breach as a privacy breach, noting in the commentary section that there was also a breach of IDR timeframes.*

Impact of Code breaches

The impact of Code breaches measures how many customers were affected by the breach and the financial impact.

Financial impact is to be considered ***prior*** to remediation activities.

> ***Example:*** If 100 customers were charged incorrect fees of $100 each due to a system error, the financial impact should be noted as $10,000; even if following identification of the breach and remediation all customers were reimbursed.

Recording breaches reported to regulators

Include regulatory breaches reported to ASIC or another regulator that were also breaches of the Code (*Table 3*).

Grading of breaches

Indicate the grading of a breach according to the severity and management action. The grading factors are detailed in *Table 3*.

Systemic breaches

Indicate whether a breach was also identified as systemic.

A systemic breach is non-compliance that has implications beyond the immediate actions and affected parties. It has affected, or is likely to affect, more than one person, and is likely to involve a process, policy or technological issue within the Code subscriber's operations.

Drop-Down Menu

Use the drop-down lists where applicable. If the drop-down list does not provide an appropriate option, use the text columns to provide explanatory comments. **DO NOT** write over the drop-down options.

Table 2 and *Table 3* provide a summary of the drop-down menu options available in the ***COB Breach Data Detail Report 2023***.

Table 2: Drop-down menu options for thematic self-reporting of breaches

Breach nature	*2022 Code section*	*2018 Code section*
Advertising and promotion	B1-B5	D1
Information about products	B6-B8	D2, D18.1
Fair Terms and Conditions	B9-B12	D4
Training Staff	B13-B14	E2
Communication	B15-B16	D15
Inclusive banking services	B17-B25	No reference
Vulnerable customers	B26-B27	No reference
Complaints resolution	B28-B34	D27, D28, D29
Account statements and balances	B35-B41	D16
Changes to account	B42-B46	D17
Term deposits	B47	No reference
Cheque accounts	B48	No reference
Joint accounts	B49-B50	D9
Subsidiary cards	B51-B52	D10
Closing accounts	B53-B56	D22
Third party products and services	B57-B58	D13, D14
Consumer credit insurance	B59-B64	No reference
Electronic communication	B65-B68	D18
Replacement of documents	B69-B75	D19
Lending	B76-B77	D6
Lending to Small Business	B78-B88	No reference

Breach nature	*2022 Code section*	*2018 Code section*
Credit cards	B89-B94	D7
Safeguards for co-borrowers	B95-B99	D11
Safeguards for loan guarantors	B100-B120	D12
Guarantors' directors	B121	No reference
Lenders mortgage insurance	B122-B125	No reference
Interest rates, fees and charges	B126-B133	D3, D5
Exchange rates and commissions	B134	No reference
Financial difficulty	B135-B143	D24
Working with representative	B144-B145	D25
Debt collection	B146-B156	D26
ePayments Code	B157	B-relationship to other Codes
Direct debit	B158-B162	D20
Chargeback	B163-B167	D21
Privacy	B168-B172	D23
Publicising Code	B173	E1
Compliance responsibilities	C180-C184	E16, E17, E19, E20
Reverse Mortgage loans	n/a	D8
Key Promises [use only in exceptional circumstances]	A1-A7	KP1-KP10

Table 3: Drop-down menu options

Breach detail	*Drop-down options*
Product/Service Type and Description **(Column D)**	• Business Finance (as per ASIC reference 1 to 8) • Consumer Credit (as per ASIC reference 9 to 22) • Guarantees (as per ASIC reference 23 to 25) • Margin Loans (as per ASIC reference 26) • Current accounts (as per ASIC reference 27 to 32) • Safe custody (as per ASIC reference 33) • Savings accounts (as per ASIC reference 34 to 39) • General insurance (as per ASIC reference 40 to 64) • Small business/farm insurance (as per ASIC reference 65 to 79) • Derivatives/hedging (as per ASIC reference 80 to 87) • Managed investments (as per ASIC reference 88 to 104) • Real property (as per ASIC reference 105) • Securities (as per ASIC reference 106 to 113) • Life insurance (as per ASIC reference 114 to 125) • Direct transfer (as per ASIC reference 126 to 136) • Non-cash (as per ASIC reference 137 to 142) • Superannuation (as per ASIC reference 143 to 178) • Traditional trustee services (as per ASIC reference 179 to 184) • Financial advice or credit assistance (as per ASIC reference 185 to 187) • Not product/service related (as per ASIC reference 188) • Other (please provide details)
Identification Method **(Column J)**	• internal process or report • random internal audit • external compliance audit • staff self-identification • customer query or complaint • other [please provide details]
Root Cause of breach **(Column L)**	• incorrect process & procedure • insufficient training • mail house error • manual error • process & procedure not followed • staffing/resourcing issues • staff misconduct • system error or failure • communication failure • 3rd party vendor • external fraud (scams) • investigation ongoing • other [please provide details]
Immediate Remedial Action **(Column R)**	• apology • ex-gratia payment • premium refund / adjustment • refund of fees/charges • review of and changes to procedure

	• review of and changes to process • review of and changes to terms and conditions • undertaking • consequence management (individual staff training) • removed / recall data • system fix • no immediate remediation required • other [please provide details]
Timeframe for immediate remedial action **(Column T)**	• immediate • within 48 hours • within 1 week • within 2 weeks • within 1 month • 1 to 3 months • 3 to 6 months • other [please provide details]
Long Term Remedial Action **(Column V)**	• financial award • refund of fees/charges • review of and changes to internal policy • review of and changes to terms and conditions • business-wide training • undertaking • business improvement • system fix • management assurance program (this can be an internal audit program) • no long term remediation required • other [please provide details]
Timeframe for long term remedial action **(Column X)**	• 6 to 12 months • 1 to 2 years • 2 to 5 years • over 5 years • other [please provide details]
Reported to Regulator **(Column Z)**	• Not Applicable (N/A) • Australian Securities and Investments Commission (ASIC) • Australian Competition and Consumer Commission (ACCC) • Australian Prudential Regulation Authority (APRA) • Australian Financial Complaints Authority (AFCA) • Office of the Australian Information Commissioner (OAIC) • Australian Transaction Reports and Analysis Centre (AUSTRAC) • Customer Owned Banking Code Compliance Committee (COBCCC) • other [please provide details]

Grading of Breach **(Column AB)**	• Grade 1 - Actions/incidents which require management attention, but do not impose a serious risk to the business operations or AFS licence • Grade 2 - Actions/incidents that require immediate management attention or an accumulation of three Grade 1 actions/incidents • Grade 3 - Actions which pose a significant risk to the business operations or AFS licence or have resulted in direct financial loss by a client (can be one incident or accumulation of 4 or more Grade 1 incidents or 2 or more Grade 2 incidents) • Grade 4 - Actions/incidents that require urgent management attention and pose a serious risk to the business operations or AFS licence (includes major compliance failures, training inadequacies and/or overall poor performance) • Grade 5 - Actions/incidents that pose a catastrophic risk to the business operations or AFS licence and are not rectifiable
Systemic Breach **(Column AD)**	• No • Yes [please provide details] • Other [please provide details]

Section D: Complaints reporting

This section of the ACS deals with complaints received during the reporting period. The following tables show how to classify complaint according to products, issues and outcomes.

Definition of Complaint

As per *AS/NZS 10002:2014* and *ASIC RG 271.27*, a complaint is an expression of dissatisfaction made to or about an organisation related to its products, services, staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.

Please note that obligations under RG 271 became effective on 5 October 2021.

Report ***all*** complaints, including complaints that are resolved to the customer's complete satisfaction by the end of the fifth business day.

Classify complaints according to the product, issue, outcome and resolution timeframe as per ASIC's IDR Data Reporting Handbook.

Products

Product categories are defined as per Tables 7 to 16 in ASIC's IDR Data Reporting Handbook.

If you cannot provide specific categorisation as per the ASIC IDR Data dictionary, use the main categories:

- *D.3.1 Business Finance (as per ASIC reference 1 to 8)*
- *D.3.2 Consumer Credit (as per ASIC reference 9 to 22)*
- *D.3.3 Guarantees (as per ASIC reference 23 to 25)*
- *D.3.4 Margin Loans (as per ASIC reference 26)*
- *D.3.5 Current accounts (as per ASIC reference 27 to 32)*
- *D.3.6 Safe custody (as per ASIC reference 33)*
- *D.3.7 Savings accounts (as per ASIC reference 34 to 39)*
- *D.3.8 General Insurance (as per ASIC reference 40 to 79)*
- *D.3.9 Derivatives/hedging (as per ASIC reference 80 to 87)*
- *D.3.10 Managed investments (as per ASIC reference 88 to 104)*
- *D.3.11 Real property (as per ASIC reference 105)*
- *D.3.12 Securities (as per ASIC reference 106 to 113)*
- *D.3.13 Life Insurance (as per ASIC reference 114 to 125)*
- *D.3.14 Direct transfer (as per ASIC reference 126 to 136)*
- *D.3.15 Non-cash (as per ASIC reference 137 to 142)*
- *D.3.16 Traditional trustee services (as per ASIC reference 179 to 184)*
- *D.3.17 Financial advice or credit assistance (as per ASIC reference 185 to 187)*
- *D.3.18 Not product/service related (as per ASIC reference 188)*
- *D.3.19 Other (please provide details)*

If a complaint involved multiple products, list them all.

Issues

Issue categories are defined as per Table 17 in ASIC'S IDR Data Reporting Handbook.

If you cannot provide specific categorisation as per the ASIC IDR Data dictionary, use the main categories:

- *D.4.1 Advice (as per ASIC reference 1 to 3)*
- *D.4.2 Charges (as per ASIC reference 4 to 13)*
- *D.4.3 CDR (as per ASIC reference 14 to 20)*
- *D.4.4 Credit reporting (as per ASIC reference 21 to 25)*
- *D.4.5 Disclosure (as per ASIC reference 26 to 30)*
- *D.4.6 Financial difficulty/debt collection (as per ASIC reference 31 to 40)*
- *D.4.7 Financial firm decision – specific to credit and lending (as per ASIC reference 41 to 44)*
- *D.4.8 Financial firm decision – general (as per ASIC reference 58 to 65)*
- *D.4.9 Instructions (as per ASIC reference 66 to 69)*
- *D.4.10 Investment performance (ASIC reference 69)*
- *D.4.11 Privacy and confidentiality (as per ASIC reference 70 to 72)*
- *D.4.12 Scams/fraud (as per ASIC reference 73 to 76)*
- *D.4.13 Service (as per ASIC reference 77 to 88)*
- *D.4.14 Transaction (as per ASIC reference 89 to 96)*
- *D.4.15 Other (please provide details)*

If a complaint involved multiple issues, list them all.

Outcomes

Outcome categories are defined as per Table 18 in ASIC Data Reporting Handbook, including:

- *Service-based remedy (ASIC reference 1)*
- *Monetary remedy, please advise total $ amount (ASIC reference 2)*
- *Contract/policy variation (ASIC reference 3)*
- *Decision changed (ASIC reference 4)*
- *Other remedy (ASIC reference 5)*
- *Withdrawn/discontinued (ASIC reference 6)*
- *Referred to another financial firm (ASIC reference 7)*
- *No remedy provided/ apology or explanation only (ASIC reference 8)*

List any outcome that does not fit into the provided categories under ‘other’ and provide additional information.

Resolution timeframes

Resolution timeframe categories are according to ASIC Regulatory Guide RG271 Internal Dispute Resolution, clause 28.3 of the 2018 Code and current obligations under section 33 of the 2022 Code, including:

- *Resolved within 21 days*
- *Resolved within 30 days*
- *Resolved beyond 30 days*

List any complaint that does not fit into the provided resolution timeframes under ‘other’ and provide additional information.

Complaints not resolved within 30 days

Provide primary reasons for complaints not resolved within 30 days.

Section E: Good industry practice

Responses to Part E.1 provide insight into how Code subscribers share values and norms. We are interested in understanding the behaviours that shape these examples and mindsets reflected in your company culture.

Online portal guidance

The online portal

The online portal is a secure system we use to collect data and receive documents when conducting monitoring activities.

Access to the online portal

Our general approach for monitoring activities is to distribute questionnaires or other information requests in Word and/or Excel format prior to the data collection period. This provides you with more time to gather the relevant information ahead of the submission date.

We will send you an email with a password and a link to the portal. The link is unique for each Code subscriber.

When you click on the link you will be asked to enter the password.

Do not share the link or the password with anyone who should not have access to the portal, or the data being submitted.

Navigating the online portal

You can navigate through the online portal using the 'Save and Next' and 'Back' buttons at the bottom of each page.

Make sure you click 'Save and Next' before navigating backwards. If you do not, you will lose the data you entered.

Saving data and returning later

You can complete part of a questionnaire and return later. Make sure you click the 'Save and Next' button at the bottom of the section to save your progress.

If you return to complete a saved activity, you will not need to enter a password again. The portal will open at the page that was last saved.

Due date

We will email you with information about the ACS and its due date. If you are unable to complete it by the date specified, please contact us as soon as possible.

Loading and saving pages

Sometimes pages may take several minutes to save, especially where there is a large amount of data or multiple attachments. You will see a 'Loading' message with a spinning circle which indicates it is still loading. If the circle stops spinning, please allow a several minutes for the page to update.

There is no specific 'time-out' period, but you should save each page regularly to ensure you do not lose your data.

Copying and pasting into the online portal

You can copy text into most response boxes. However, please note that if you are required to complete data tables you may need to complete fields within a table manually.

Uploading supporting documents

If you are reporting a breach of the Code, you are required to upload a copy of your Breach Data Details Report into the portal. Please click 'Browse,' select the required document from your computer, click 'Open' and then 'Submit.'

If you need to upload more than one document, or the document is not a Word, Excel or PDF file, please create a zip file containing the documents and then upload the zip file.

In most cases, you can create a zip file by selecting the relevant documents, right-clicking and selecting 'Send to' > 'Compressed (zipped) folder.'.

Submitting ACS

At the end of the questionnaire, you will be asked to re-enter your password. On the subsequent page there is a 'Submit final response' button. Clicking on this button will transmit the data to us.

There will be no opportunity for you to amend the data after it has been submitted, so make sure it is correct.

If you think the information, you submitted may be wrong, contact us immediately.

Saving a record of the submission

Once you submit, you will be able to download a PDF copy of your submission.

The PDF will show the filenames of documents you uploaded, but not the contents of those documents.

Online portal security

The portal is a third-party application provided by The Evolved Group. The Evolved Group was formally audited in February 2022 by Best Practice Certification and received ISO 27001:2013 (Information Security Management System Requirements) accreditation.

Contact us

If you have any difficulties or any queries, please contact:

- Daniela Kirchlinde, Code Compliance and Operations Manager, dkirchlinde@codecompliance.org.au
- Tania Meadows, Senior Compliance Analyst, tania.meadows@codecompliance.org.au mailto: