CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

ACS VERIFICATION REPORT 2019–20

INSIGHTS AND LEARNINGS

31 May 2021

Contents

Message from the Chair

I am pleased to present the 2019–20 Annual Compliance Statement (ACS) Verification Report of the Customer Owned Banking Code Compliance Committee (the Committee).

In 2019–20, Code subscribers self-reported 2,537 breaches.[1]

This report is based on discussions between staff on behalf of the Committee with 25 Code-subscribing customer owned banking institutions that participated in our ACS Verification Program.

It provides in-depth coverage of subscribers' reporting of Code compliance, along with examples of better industry practice, and guidance and recommendations from the Committee on areas where the reporting indicates that compliance could be improved.

In recognition of the significant and unprecedented operational challenges faced by Code subscribers during the 2019–20 reporting period due to the COVID-19 pandemic, the Committee gave subscribers additional time to complete their 2019-20 ACS questionnaire.

This has resulted in this year's ACS Verification Program concluding later than normal. Accordingly, the findings are presented separately in this report, rather than being included in our Annual Report.

The discussions with Code subscribers have helped shape the structure and content of this report.

The connection between high reported breach numbers and solid compliance frameworks

The Committee noted a distinct connection between the volume of breaches an institution self-reports and the strength of their compliance frameworks.

We found that institutions that reported high breach numbers generally appear to have in place solid Code compliance frameworks that include effective breach detection mechanisms, auditing and monitoring functions, and appropriate compliance training for their staff. Many also spoke of having more closely monitored compliance with specific Code obligations, such as responsible lending practices and customer privacy, and in some cases, this has led to higher levels of reported breaches in these areas.

Conversely, institutions that reported low breach numbers were found to have less rigorous breach identification and reporting processes, as well as staff who are less aware of their Code compliance obligations.

Far from indicating complete Code compliance, an institution repeatedly self-reporting no breaches is highly likely to have inadequate processes, procedures and systems, and staff that are neither encouraged nor supported to self-report Code breaches.

[1] See page 12 of the COBCCC Annual Report 2019-20 https://www.cobccc.org.au/app/uploads/2020/12/COBCCC-Annual-Report-2019-20.pdf

Any institution that reported nil breaches in 2019–20 is urged to review its compliance frameworks and ensure that staff across the business understand their Code compliance obligations and the importance of recording and reporting all breaches.

Issues with the ACS reporting process

Discussions with subscribers about the accuracy of their data revealed some confusion and misunderstanding around the reporting requirements of the ACS and Breach Data Report.

In one example relating to the financial impact of Code breaches, subscribers said they understood the term “financial impact” to mean the amount outstanding once remediation had been paid to the customer, rather than the pre-remediation amount.

In another example, several institutions were found to have reported all customer service incidents as breaches without first determining whether or not they constituted a breach of the Code, which led to overreporting for the 2019-20 period.

The Committee is reviewing the instructions for completing the Breach Data Report in light of this feedback.

Responding to vulnerable customers

The Committee asked each of the participants in the ACS Verification Program to share their strategies for identifying and dealing with customers in vulnerable circumstances.

We were encouraged to learn that institutions of all sizes are working to ensure that the protection of vulnerable customers, including older people and those experiencing financial hardship, is front of mind across the business.

Many are actively increasing staff awareness of vulnerability via focused training programs and supporting staff to respond to vulnerable customers with sensitivity and compassion.

Some have appointed a dedicated Vulnerable Customer Advocate to assist vulnerable customers when dealing with the institution. Others are leveraging technology to protect vulnerable customers from financial scams and fraud.

We hope to see every customer owned banking institution take inspiration from the examples we share in this report.

Business continuity during the COVID-19 pandemic

It appears that Code subscribers responded well to the COVID-19 pandemic. From the outset, institutions diverted staff from across the business to customer service and financial hardship teams to help respond to the increasing number of requests for loan deferrals and financial hardship assistance and to answer general enquiries.

Many institutions took a personalised approach to helping customers, contacting or visiting them to discuss their specific needs and offer assistance.

The Committee hopes that all institutions provide an appropriate level of individualised care and support for their customers and local communities, even as Australia recovers from the economic and social impacts of COVID-19.

Appreciation

I take this opportunity to thank the 25 institutions that were involved in the 2019–20 ACS Verification Program. The Committee appreciates their willingness to discuss the challenges that they and the industry as a whole are facing, as well as their receptiveness to our feedback on ways to improve their breach data reporting.

Looking ahead, the Committee's plans are that ACS verification conferences will be able to be conducted with all Code subscribers on an annual basis.

Jocelyn Furlan

Jocelyn Furlan

Independent Chair
Customer Owned Banking Code Compliance Committee

About this report

This report provides a detailed analysis of the findings of the 2019–20 Annual Compliance Statement (ACS) Verification Program. It includes the Committee's observations on the overall Code compliance of the customer owned banking sector, as well as guidance and recommendations for institutions on how to improve their compliance reporting and achieve better practice within their organisation.

It follows on from our 2019–20 Annual Report,[2] which was published in December 2020 prior to the completion of the 2019–20 ACS Verification Program. This report provides more detail in relation to the Program.

Purpose of the ACS Verification Program

The Committee's Compliance Manager[3] undertakes the ACS Verification Program each year which includes a series of conferences with a sample group of Code subscribers to validate their breach reporting and gain insights into the day-to-day management of their Code compliance obligations (see below under 'Methodology' for more detail about this).

The aim of the program is for the Committee to hear directly from subscribers about:

- the story behind their data
- the context for their reported breach numbers
- how they identify and respond to breaches of the Code
- any emerging trends
- their strategies for improving their overall Code compliance
- any examples of good practice that can be shared with the industry.

The program also provides Code subscribers with the opportunity to:

- raise with the Compliance Manager any concerns they may have about the ACS process
- receive feedback and guidance from the Committee about completing their ACS
- review and improve their compliance monitoring and breach data reporting
- identify any emerging risks or issues.

Methodology

In previous years, ACS verification conferences have been conducted with a sample group of around 20 customer owned banking institutions, representing approximately one-third of all Code subscribers. Under this arrangement, each group takes part in the ACS Verification Program every three years to give the Compliance Manager the opportunity to engage regularly with all institutions about their ACS and breach data reporting.

[2] www.cobccc.org.au/app/uploads/2020/12/COBCCC-Annual-Report-2019-20.pdf
[3] For information on the operations of the Committee see **Appendix 3**.

This year, the Committee extended the program to include more Code subscribers, bringing the total to 25. Most participants last took part in the program in 2017 and represented a range of locations and business sizes, including:

- 13 Category A institutions (over $2b in assets)
- 5 Category B institutions (between $1b and $2b in assets)
- 4 Category C institutions (between $500m and $1b in assets)
- 2 Category D institutions (between $200m and $500m in assets)
- 1 Category E institution (under $200m in assets).[4]

The ACS verification conferences provide a good opportunity for the Compliance Manager to meet with senior staff from Code-subscribing institutions and it was encouraging to see a cross-section of employees represented at the conferences this year, including staff from Legal and Compliance Departments and Complaints Departments, as well as Chief Risk Officers and other departmental heads.

From the Committee's viewpoint, we appreciate being able to gain a better understanding of institutions' breach data, complaints reporting and monitoring mechanisms and to provide them with guidance and support in these areas. It is hoped that this guidance and support, along with our feedback for improving the ACS and breach data reporting process, are shared with institutions' Boards and Executive Management teams.

[4] Further detail about participating Code subscribers can be found in **Table 1 Appendix 1**.

Identification and reporting of Code breaches

Code subscribers are required to self-report Code breaches to the Committee each year via the ACS. The information we receive from institutions about how and why they have breached the Code helps us identify current and emerging risks, as well as provide guidance on better industry practice.

In recent years, we have seen a large variance in reporting culture, with some Code subscribers self-reporting multiple breaches and others self-reporting nil breaches. In 2019–20, one Code subscriber self-reported 636 breaches while 16 Code subscribers self-reported nil breaches. There was also a significant variance in the number of breaches self-reported by Category A Code subscribers: one subscriber reported more than 500 breaches, while another reported nil breaches.

The Committee's aim in discussing breach reporting with the institutions that participated in the ACS Verification Program was to establish why there are such reporting inconsistencies each year and to better understand the following:

- How do institutions identify and record Code breaches?
- What breach reporting mechanisms do they have in place?
- What actions do they take to remediate Code breaches?

Better reporting processes led to higher breach reporting

All Code subscribers that participated in the 2019–20 ACS Verification Program spoke of having a positive breach reporting culture, whereby staff are encouraged to report Code breaches, and there are systems and processes in place to support breach reporting and monitoring. However, we identified distinct differences in the processes put in place by subscribers reporting higher and lower volumes of breaches.

Those who self-reported a higher number of breaches during the year generally appear to have rigorous breach identification, recording and reporting processes, backed up by compliance training for their staff. These processes and procedures were less common among those who self-reported lower breach numbers.

One Category A institution, which self-reported 57 Code breaches in 2019–20, has implemented a specialised "hindsight" team to strengthen the first line of defence. Part of the team's role is to review all loans each quarter. This review resulted in the detection of 44% more breaches of the Code's responsible lending obligations compared to the previous reporting period. The institution also uses

The benefits of breach reporting

If subscribers report increased numbers of Code breaches, it demonstrates that they:

- *take their auditing and monitoring functions seriously*
- *have breach detection mechanisms that are effective*
- *have a strong compliance culture that encourages breach reporting across the organisation*
- *are well placed to remediate the breach and prevent it recurring.*

We encourage all customer owned banking institutions to review their Code compliance obligations and improve their breach reporting to ensure they identify, remediate and learn from each Code breach.

a Quality Assurance process to undertake a ‘deep dive’ into any compliance issues and has focused on building a psychologically safe reporting culture, where staff are encouraged to self-report instances of non-compliance.

Another Category A institution replaced its previous breach reporting process, which required manual entry of all breach data, with an upgraded breach reporting system that is now accessible to staff across the organisation. This has led to improved breach reporting by all staff and improved the quality of breach data. It has also resulted in the institution self-reporting twice as many Code breaches as the previous year (74 in 2019–20 compared to 37 in 2018–19).

A third Category A institution identified several breaches that impacted multiple customers (in one case, a single Code breach impacted 423 customers). In an example of good breach awareness by all staff within the organisation, some of the breaches were identified by areas other than Compliance, including Lending, Marketing & Digital and Financial Planning. This led to the institution being able to quickly rectify the issue and remediate all affected customers.

Conversely, one Category C institution explained that the reason it did not identify any Code breaches in 2019–20 was due to a lack of awareness amongst its staff about how to define and report a breach. The institution is working to resolve this issue by migrating to an online incident reporting system that will be more accessible to staff and link back to the Code.

Good process supported by a positive reporting culture

One Category A institution described a two-step process for identifying breaches of the Code.

In Step 1, front-line staff report an incident to the Risk & Compliance team. In Step 2, the Risk & Compliance team assess the incident to determine if there has been a breach of the Code.

All incidents are reviewed quarterly by the Risk & Governance Committee and the process is underpinned by tight breach reporting timeframes and a top-down organisational culture that encourages staff to report breaches.

The pros and cons of breach registers

Asked about their breach reporting mechanisms, many of the Code subscribers who self-reported low numbers of breaches said they record breaches and incidents in a register, which is then reviewed by senior leaders within the organisation.

One Category B institution, which has self-reported three Code breaches each year since 2017–18, said it makes the reporting register accessible to all staff and promotes a positive culture of awareness through training and policy.

Another subscriber – a Category A institution that self-reported three Code breaches in 2019–20 – said breaches are often identified through complaints data and recorded in a complaint register, which is periodically reviewed.

Recording instances of non-compliance in a breach register should be considered one part of a wider breach reporting process that includes investigating the root cause, remediating the breach and sharing any learnings with staff across the business to prevent a recurrence.

Breach registers appear to be most effective when dedicated Risk and Compliance staff are given accountability for managing them. One Category B institution told the Committee that most of the 15 Code breaches self-reported last year were identified by its Risk and Compliance team through a process that involves all staff members being able to log an incident in the register. Once logged, the incidents are triaged by the Risk and Compliance team to determine if there is also a Code breach.

Recommendations

Based on the findings from the interviews, it appears that many Code subscribers have processes in place to support a positive reporting culture. Where institutions identified a Code breach, they generally demonstrated a constructive approach to investigating the cause, taking remedial action through system fixes and process improvements, and updating policies and procedures to prevent future occurrences.

All subscribers – particularly those who consistently report few or no Code breaches to the Committee – should consider the following recommendations for better breach reporting outcomes:

- Foster a positive reporting culture within the organisation.
- Communicate the expectation that Code breach reporting is the responsibility of all staff, not just the Compliance & Monitoring teams.
- Ensure that all incidents reported via a breach register are reviewed by accountable senior members of staff.
- Encourage the reporting of breaches to the Board, which should have oversight of all breaches and incidents.
- Provide Code-specific training to staff so that they can confidently identify incidents that could indicate non-compliance with the Code. Ensure they understand the Code's role in the consumer protection framework and the importance of all staff meeting their Code obligations to customers.

Impact of Code breaches

As part of the annual breach reporting process, subscribers are required to give the Committee information about the impact of any Code breaches, including the number of customers affected and the resulting financial impact.

In 2019–20, subscribers reported that around 821,000 customers[5] were affected by 2,537 Code breaches. The resulting financial impact to these customers was estimated to be a little over $470,000. A large number of breaches were reported by subscribers as having $0 financial impact on the affected customers, while almost a quarter of the total financial impact ($100,000) involved just two individual customers, each affected by a single Code breach.

Given the high number of reported breaches and customers affected, the Committee would have expected the total financial impact to be higher. Code breaches can have a significant financial impact on customers, and we were concerned that Code subscribers were not accurately recording the financial impact of each breach on the affected customers.

Accordingly, the Compliance Manager raised these concerns with the 25 Code subscribers that participated in the ACS Verification Program and reviewed each institution's Breach Data Report in consultation with them to determine any issues.

Interpreting financial impact

Through these discussions, it became apparent that there was a misunderstanding around the definition of "financial impact". In asking for the total financial impact of each breach, the Committee expected subscribers to provide figures based on the financial impact to customers before any remediation.

Subscribers explained, however, that they had understood financial impact to mean the amount that was outstanding once remediation had been paid to the customer. This was why subscribers reported breaches as having $0 financial impact to customers.

In response to subscribers' suggestions, the Committee will amend the financial impact definition in the Breach Data Report instructions to clarify that financial impact should be reported as the pre-remediation figure, not the amount outstanding once remediation has been paid.

Issues with the Breach Data Report

Further discussion about the Breach Data Report revealed some confusion among subscribers about how to complete the Excel spreadsheet – namely, what information the Committee expects subscribers to include in each column.

We remind subscribers that the purpose of the Breach Data Report is to identify Code breaches, investigate their root cause and explain what remedial actions have been undertaken. To make

[5] Numbers are indicative only, as not all Code subscribers provided conclusive information for each self-reported Code breach.

completion of the Breach Data Report more straightforward for institutions, we have put together the following tips.

Key tips for completing the Breach Data Report

Describe the incident

- Provide as much information as possible about the breach incident. Be descriptive. Help the Committee understand what happened. Explain in detail the set of facts that led to the reported Code breach occurring.
- Do not treat the Breach Data Report as a data dump exercise by copying and pasting the customer's information into the spreadsheet. The Committee should not be provided with any personal information about the customer, including their name, contact details or account numbers.

Provide information about the root cause

- Each row of the Breach Data Report spreadsheet should reflect one root cause. This might be one incident that impacted a number of customers. For example:

  An IT failure prevents disclosure documents being sent out to 100 customers. This should be registered as one Code breach that affected 100 customers, with the root cause recorded as an IT failure.

Record the financial impact

- Provide figures based on the financial impact to customers before they received any remediation. For example:

  A staff member accidentally deposits Customer A's money into Customer B's account. The incident is remediated when the money is removed from Customer B's account and deposited into Customer A's account BUT – the financial impact will be the amount of the incorrect deposit.

Detail the immediate and long-term remedial action

- Explain in detail what you did to fix the breach. What immediate action did you take when the breach was identified? What long-term solutions did you implement to prevent further breaches? Listing these can help you spot emerging issues or risks within your organisation. For example:

  If multiple employees fail to follow a particular policy, this may be a sign that the policy is unclear and needs amending or that staff need training in the policy.

Understanding of Code breaches for specific Code obligations

One of the Committee's key purposes in conducting the ACS Verification Program with Code subscribers is to ascertain how they identify, record, report and respond to breaches of specific areas of the Code.

This helps the Committee to:

- understand how customer owned banking institutions interpret particular Code obligations
- understand how they measure their compliance with those obligations
- provide guidance, where necessary, on issues with their breach reporting and/or interpretation of certain Code provisions
- identify any trends and emerging risks.

In 2019–20, the highest number of self-reported Code breaches were spread across eight Code provisions:

- Key Promise 5 – Delivering high customer service
- Key Promise 8 – Complying with legal obligations
- Section D2 – Product information
- Section D3 – Interest rates, fees and charges
- Section D16 – Statement of accounts
- Section D6 – Responsible lending
- Section D23 – Information privacy and security
- Section D1 – Advertising.[6]

Accordingly, discussions with subscribers were focussed in these areas. In some cases, we sought to understand why a particular institution reported multiple breaches of a specific Code obligation. In other cases, we were aiming to find out why a specific Code obligation was the subject of breaches by numerous institutions. The outcome of these discussions, along with some examples of better practice by various institutions, are provided on the following pages.

Customer service (Key Promise 5)

Obligation

Key Promise 5 – We will deliver high customer service and standards

We will issue and distribute products and provide services that are useful, reliable and of value to our customers. We will make sure our staff and agents or representatives are well trained. We will promote secure and reliable banking and financial services and keep you up to date on any changes to the products and services we provide to you. We will treat your personal information as private and confidential.

[6] Detailed analysis of the breaches of these Code obligations can be found in Table 2 Appendix 2 of this report.

A snapshot of customer service breach reporting

There were 749 self-reported breaches of Key Promise 5 (‘We will deliver high customer service and standards’) in 2019–20, representing 30% of all Code breaches for the year. In terms of customer impact, breaches of this Key Promise affected the highest number of customers (267,167) and had the greatest financial impact ($177,844).

The vast majority (83%) of all customer service breaches were self-reported by three Category A institutions, one of which, alone, accounted for 51%. Of the remaining breaches, 15% were self-reported by seven other Code subscribers.

Overreporting caused high customer service breach numbers

From our discussions with Code subscribers about their breach data, the Committee learnt that some institutions were automatically reporting customer service incidents as Code breaches. This has resulted in an overreporting of breaches.

In its verification conference, the Category A institution responsible for more than half of all breaches of Key Promise 5 advised that its breach numbers were high because it self-reports all customer service incidents as Code breaches.

Rather than conduct a triage of the incidents to assess whether they are also Code breaches, the institution copies all customer service incidents from its breach register into the Breach Data Report. In response to our feedback, the institution has agreed to improve its processes for determining whether customer service incidents are also Code breaches.

A second Category A institution, which accounted for almost 20% of all self-reported customer service breaches in 2019–20, also included a high number of incidents in its breach reporting. This resulted in the institution self-reporting three-and-a-half times more customer service breaches than the previous year.

The institution explained that it had seen a general increase in the reporting of risk incidents in 2019–20. These risk incidents were automatically reported as breaches, resulting in breach numbers being overreported. Its Risk and Compliance team has responded by improving training in Code competency and awareness within the organisation so that staff have a better understanding of the difference between an incident and a Code breach.

The Committee appreciates that Code-subscribing institutions may have different interpretations of what constitutes a breach of customer service. Nonetheless, to avoid overreporting breach numbers, we recommend closely reviewing each incident to determine whether it is in fact a breach of the Code’s customer service obligations before self-reporting it to the Committee.

Manual error as a ‘catch all’ breach cause

Manual error by staff was the top reason given by subscribers for instances of non-compliance across almost all areas of the Code in 2019–20 but particularly for breaches of Key Promise 5.

One Category A institution self-reported a high number of customer service breaches after discovering that some of its call centre staff were providing customers with incorrect advice. The institution analysed each breach to determine any patterns or trends in the errors made and responded by improving relevant processes and upskilling staff.

The Committee is aware that institutions often select manual error as a 'catch all' as the root cause of reported Code breaches. In light of this, we would encourage those with high numbers of breaches caused by manual error to dig deeper into the root cause and find out why the error occurred, how it led to a breach and what remedial actions need to be taken to prevent a recurrence.

Privacy (Key Promise 8 and Section D23)

Obligations

Key Promise 8 – We will comply with our legal and industry obligations

We will be responsible, prudent managers of our institution, and will comply with all our obligations under the law and relevant codes of practice. We will act fairly and consistently with good banking and financial service industry practice.

Section D23 – Information privacy and security

23.1. We will comply with the Privacy Act 1988[7] and the Australian Privacy Principles[8], including with respect to credit reporting and the collection, storage, use and disclosure of your personal and financial information.

A snapshot of privacy breach reporting

Breaches of the Code's privacy obligations, set out in Section D23, accounted for 31% of all self-reported breaches in 2019–20, making privacy the top breach category overall. Between them, 33 institutions self-reported 783 privacy breaches, with one Category A institution accounting for 446 breaches (57% of all Section D23 breaches) and two other institutions reporting more than 100 breaches each.

Breaches of Key Promise 8, under which Code subscribers mainly self-reported breaches regarding privacy obligations to customers, was the third-most breached category. There were 307 breaches of this Key Promise (12% of the total) reported by 20 institutions. More than half were self-reported by just two Category A institutions. Another quarter were self-reported by four institutions (three Category A and one Category C).

There were high numbers of customers impacted by breaches of both Section D23 and Key Promise 8. Breaches of Section D23 affected 253,356 customers and had a total financial impact of $540, while breaches of Key Promise 8 affected 27,151 customers and had a more significant financial impact totalling $50,718.

Institutions named manual error as the main root cause for privacy breaches, with a failure to follow processes and procedures as the second most cited root cause.

[7] www.legislation.gov.au/Series/C2004A03712
[8] www.oaic.gov.au/privacy/australian-privacy-principles

Greater focus on privacy leads to better breach identification

Several institutions explained that improved systems and processes, along with a sharper focus on customer privacy throughout the organisation, led to more privacy breaches being identified and reported in 2019–20.

One Category A institution self-reported three times more privacy breaches than the previous year. Following a system upgrade, the institution identified that its processes for removing account holders from joint-signatory accounts did not reflect customers' instructions, resulting in breaches of the Code's privacy obligations. The institution has since improved its processes and provided appropriate training to relevant staff members.

Appointing a privacy officer

*Two Category A institutions have appointed a dedicated **privacy officer** who sits within the Compliance team. The privacy officer's role includes:*

- *managing the privacy framework (including all processes, systems and controls)*
- *assessing the treatment of customers' personal information*
- *reviewing all incidents reported in the breach register to determine whether they are a breach of the Code's privacy obligations*
- *embedding privacy impact statements within the business*
- *training staff throughout the business on privacy and data issues.*

One of the two institutions has seen a 37% increase in privacy breaches since the Privacy Officer was appointed. This indicates that Code breaches are being identified, remediated and reviewed for any patterns or trends to avoid a recurrence.

A second Category A institution said that the Committee's 2020 Own Motion Inquiry report, *Compliance with privacy obligations follow-up inquiry outcomes*,[9] had prompted a close examination of whether the institution was meeting the Code's privacy requirements. This led to the identification of 61 privacy breaches – almost twice as many as the previous year – and has resulted in front-line staff taking a more active role in ensuring that customers' privacy is protected in line with the Code obligations.

One institution, which accounted for almost half of the privacy breaches reported by Category C Code subscribers, attributed a significant uptick in privacy breaches (from 3 in 2018–19 to 59 in 2019–20) to an increased focus on its procedures and processes for updating personal information.

Some high breach numbers were caused by incorrect reporting

Two Category A institutions with high breach numbers were found to have made errors in their reporting.

One self-reported a third of all breaches of Key Promise 8 after a bug in the system prevented customers from completing all information when opening an account. The institution mistakenly self-reported this as 70 breaches of Key Promise 8 impacting 70 customers, when it should have been reported as one breach (with a single root cause) impacting 70 customers.

[9] www.cobccc.org.au/app/uploads/2020/06/COBCCC-OMI-Privacy-June-2020.pdf

The other institution self-reported twice as many privacy breaches as the previous year when it mistakenly reported both primary and secondary breaches for the same incident.

Recommendations

The Committee noted that some interviewed subscribers are taking a proactive approach to ensure compliance with the *Privacy Act* and the *Australian Privacy Principles*, as stated in Section D23 of the Code.

For example, some subscribers have appointed a dedicated privacy officer, support front-line staff to take an active role in identifying and reporting privacy breaches, and provide training on privacy information and security to staff across the organisation.

The Committee encourages all Code subscribers to consider adopting these practices.

We also remind subscribers to review the recommendations and checklist provided in our 2018 Privacy Own Motion Inquiry report[10] and our follow-up 2020 report[11] for additional guidance.

Provision of Information (Key Promise 3, Section D2 and Section D3)

Obligations

Key Promise 3 – We will give you clear information about our products and services

We will provide clear and accessible information about our products and services, so you can make an informed decision about the product you want. We will disclose interest rates, fees and charges in an accessible and clear format and provide you with regular account statements. We will give you information on how to minimise fees and charges. Our advertising and promotional material will not be misleading.

Section D2 – Information about our products

2.1. We will make general information about our products and facilities readily available to anyone who wants it. This information will be:

- clear, concise and accurate
- written in plain language
- generally sufficient to allow you to make an informed decision about the product or facility, and
- consistent with any applicable legal requirements.

2.2. We will make a copy of the standard Terms and Conditions applying to a product or facility available to you, if you ask us. We will not require you to apply for the product or facility first. However, depending on our product range and systems, we may need to ascertain

[10] www.cobccc.org.au/app/uploads/2018/06/COB-OMI_Privacy-26June2018.pdf
[11] www.cobccc.org.au/app/uploads/2020/06/COBCCC-OMI-Privacy-June-2020.pdf

the features or characteristics of the product you are considering before we are able to generate a copy of standard Terms and Conditions for that product.

2.3. We will answer any questions you have about the features of our products and facilities and how they work.

Section D3 – Information on interest rates, fees and charges

3.1. Interest rates and fees and charges applying to our products and facilities will be readily available to anyone who wants this information. The information will be clear, concise and up-to-date.

3.2. In the case of products with variable interest rates, we will tell you what the current rate is when you apply for the product. We will also use a range of methods to publicise our rates. We will answer any questions you have about our interest rates and how they are calculated and applied.

3.3. Our information about fees and charges will cover all applicable fees and charges, including non-standard fees that only apply in particular situations (e.g. fees if you overdraw your account or are late in making your payments). We will also make general information available on how to avoid or minimise fees and charges. We will answer any questions you have about the fees applying to a product or facility. We will regularly review the effectiveness of our disclosure of fees and charges to customers.

3.4. We will inform you of any fee for a one-off service (e.g. issue of a bank cheque), before you become liable to pay it.

A snapshot of breach reporting on the provision of information

Compared to the previous reporting period, in 2019–20 we saw a slight uptick in self-reported breaches relating to the provision of accurate and efficient information about interest rates, fees and charges (D3 – 5%) and products (D2 – 4%). Sixteen per cent of customer complaints centred around charges, while another 6% of complaints related to disclosure issues.

Of the breaches concerning product information, over half (56% of 111) were self-reported by two Category A institutions. One of these self-reported 41% while the other self-reported 15% of the total. Just over a third of all breaches concerning interest rates, fees and charges were self-reported by two Category A institutions.

In terms of customer impact, breaches of all three Code sections affected 74,768 customers and had a total financial impact of $61,664.

Providing customers with incorrect information

One Category A institution self-reported 40.5% of all information-related breaches. The institution explained to the Compliance Manager that the breaches were caused by a staff member providing customers with incorrect product information. The breaches were identified through recordings of the staff member’s phone conversations with customers.

Responsible Lending (Key Promise 4 and Section D6)

Obligation

Key Promise 4 – We will be responsible lenders

We will lend responsibly and will try to assist you if you find yourself in financial difficulties.

Section D6 – Responsible lending practices

6.1. We will always act as a responsible lender and will comply with responsible lending laws.

6.2. We will base our lending decisions, including decisions to extend existing credit facilities, on a careful and prudent assessment of your financial position and requirements and objectives as indicated to us. We will periodically review our credit assessment procedures and criteria for the products we issue.

6.3. We will generally only lend amounts to you that we believe, on the information available to us, you can reasonably afford to repay. However, different criteria will apply in the case of some products, such as bridging finance arrangements and reverse mortgage loans (if we offer these).

6.4. We expect you to provide honest and accurate information to us when applying for a loan or the extension of a credit facility. We will also take reasonable steps to verify your financial situation.

6.5. We will promote the responsible use of credit to our customers using a range of approaches.

A snapshot of breach reporting relating to responsible lending practices

Breaches of Section D6 and Key Promise 4 accounted for just under 4.5% of all self-reported breaches in 2019–20. These breaches affected a total of 389 customers and resulted in a financial impact of $71,597 – the second highest financial impact for the reporting period.

Over two-thirds (69% of 105) of breaches concerning responsible lending practices were self-reported by four Code subscribers. One of these – a Category A institution – accounted for one-third (33%) of the reported breaches.

Subscribers say improved monitoring of lending practices is leading to better breach identification

In their interview with the Compliance Manager, many Code subscribers stated that responsible lending practices have become a key area of focus for them following the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry. According to these subscribers, this is leading to better identification of incidents and breaches relating to the Code's responsible lending practices.

The Committee was unable to validate this statement from the information subscribers provided in the ACS and the verification interviews. However, the examples below indicate that some subscribers, at least, are implementing stricter auditing and monitoring of their lending practices.

The Category A institution that self-reported one-third of all responsible lending breaches has implemented monitoring processes, including internal audits and monthly file reviews, with a particular focus on new staff members' files. These processes helped the institution detect a number of breaches that occurred when loans staff members failed to follow the correct procedure for verifying a borrower's income (for example, not collecting sufficient pay slips).

A Category C institution, which reported around 14% of all responsible lending breaches, detected the breaches via a hindsight review that found issues with a sample of loans that had been approved via a manual process. The institution advised the Committee that it has since invested in a digital data scraping tool that automates the loan approval process, providing consistent reporting and removing ambiguities and inefficiencies.

In the case of a Category B institution, it proactively identified an incorrect system code affecting the redraw facilities of 145 customers. While the issue was detected and fixed before any of the customers were financially impacted, the institution correctly self-reported this as a single breach impacting 145 customers.

Reviewing the lending process end to end

One Category B institution carries out an end-to-end review of the lending process with the loans team.

As part of this process, it conducts workshops with various departments and has implemented a variety of automated checklists to ensure a more efficient and better customer experience.

This has contributed to the prevention of Code breaches relating to responsible lending practices.

Account statements and balances (Section D16)

Obligation

Section D16 – Account statements and balances

16.1. We will provide you with regular account statements clearly setting out all transactions relating to your deposit and loan accounts with us. Where you elect to have your account statements sent by post, we will send your statements to the last address you have given us, unless we reasonably believe that this is no longer your correct address. (The provision of account statements electronically is considered in section 18).

16.2. Account statements will be sent or made available at least every 6 months. We will provide you with more frequent periodic account statements if you request these. We will also comply with our obligations in relation to account statements under consumer credit and other applicable laws.

16.3. Account statements will include clear information about our fees and charges incurred on your account during the statement period. Fee amounts will not be bundled but will be broken down by transaction type and channel. The impact of any applicable fee-free limit or rebate scheme will also be indicated.

16.4. We will provide a simple method(s) of access for you to find out the balance on your account. We will not impose any fees for using this access method.

16.5. This section does not apply to:

- passbook accounts, and
- accounts that are dormant.

A snapshot of breach reporting relating to statement of accounts

There were 89 breaches concerning account statements and balances in 2019–20. Almost three-quarters of those breaches were self-reported by one Category E institution. In our discussions with Code subscribers, the Committee sought to discover how their statement of account breaches were identified.

After not reporting a single statement of account breach in 2018–19, the Category E institution mentioned above, self-reported 64 breaches in 2019–20 as a result of a misunderstanding in how to complete the Breach Data Report. The breaches occurred when a system error prevented customers who had closed their accounts from being issued with online statements. As all the breaches had the same root cause, the Committee advised the institution that it should have reported a single breach that impacted 64 customers, rather than 64 individual breaches.

In the case of one Category B institution (which accounted for 40% of all statement of account breaches amongst subscribers of that size), a third-party provider sending out information to customers on the institution's behalf was found not to have sent customers a required email notification. Once the breach was identified, the institution worked with the provider to ensure that their systems were updated and tested.

Advertising Breaches (Section D1)

Obligation

Section D1 – Advertising

1.1. We will ensure our advertising and promotional material is not misleading or deceptive. We will not mislead or deceive you either by what we say or represent, or by omission (what we fail to say or represent). We will have regard to ASIC regulatory guidance about advertising financial products and services including credit when developing and reviewing our advertising and promotional material.

A snapshot of advertising breach reporting

Between them, 13 institutions self-reported 43 breaches of the Code's advertising obligations in 2019–20. Almost half (42%) of these breaches were self-reported by one Category A institution.

Organisation-wide awareness of the Code

This high-reporting Category A institution advised that most of its self-reported breaches came to light as a result of complaint and audit monitoring and were identified by staff in the Marketing Department. This indicates that a range of staff within the organisation are aware of their Code obligations and that the institution is not relying solely on the compliance/audit function to detect and report Code breaches.

Identification and reporting of complaints

A total of 27,041 complaints were self-reported in 2019–20, with 95% of all Code subscribers self-reporting at least one complaint. Of all complaints received during the year, just 1.4% were identified by subscribers as also being a Code breach. The Committee does not audit subscribers' data, so these figures have not been verified and only reflect subscribers' self-reporting.

As the nature of customer complaints and the way subscribers resolved them were covered in the Committee's 2019–20 Annual Report, [12] complaints were not a key area of focus of the ACS Verification Program. Where the Committee identified an issue with individual Code subscribers' complaints reporting, we raised it with them during the verification conference and provided feedback.

For example, one Category A institution advised that it does not currently capture the outcome of complaints as per definitions requested in the ACS. As a result, all complaints were listed under the outcome category 'other'.

The subscriber stated that complaints were resolved by working with the customer to achieve the best solution for all parties involved, including providing the customer with avenues for escalation of the complaints (e.g. referral to AFCA). The institution confirmed that in transitioning to the new Regulatory Guide 271, it will begin capturing this information as part of the data reporting requirements from October 2021.

Better resourcing improves dispute resolution timeframes

One Category A institution identified an issue with the length of time it was taking to resolve internal and external disputes within its contact centre.

To resolve the issue, the institution deployed a specialised team which separated the case work into internal dispute resolution cases and external dispute resolution cases, resulting in a significant reduction in dispute resolution timeframes across the board.

Code breaches identified via complaints

As part of the complaints reporting process, subscribers are required to provide the Committee with the number of complaints they received that also resulted in the identification of a Code breach. Furthermore, we expect subscribers to include all Code breaches identified through customer complaints in their overall breach numbers for the reporting period, and to provide an explanation in the Breach Data Report for why they considered a Code breach occurred.

Recommendations

To ensure that they record all Code breaches, subscribers are encouraged to cross-check their complaints data with their breach data. Where a complaint also identifies a Code breach, this breach should be self-reported along with all other Code breaches, and an explanation provided in the Breach Data Report.

[12] Further analysis of the issues and products that were the focus of most customer complaints, as well as how subscribers resolved these complaints, can be found in our 2019–20 Annual Report. **Table 3 in Appendix 2** of this report also provides analysis of high volumes of self-reported complaints for the reporting period.

Likewise, if a subscriber lists the identification method for a Code breach in the Breach Data Report as “customer” or “customer complaint”, this should be reflected in the subscriber’s complaints data.

As mentioned elsewhere in this report, the Committee encourages customer owned banking institutions to adopt a strong incident reporting culture.

Understanding vulnerability

As part of the 2019–20 ACS, Code subscribers were asked about their compliance monitoring activities in relation to vulnerable customers.

The majority of institutions across all size categories reported having conducted compliance reviews on responsible lending obligations involving vulnerable customers and dealing with customers in financial difficulty. Most subscribers in Categories B to E also said they reviewed their compliance with the Code's obligations for identifying and assisting customers affected by elder abuse.[13]

To gain a more complete picture of these activities, the Committee asked each of the participants in the ACS Verification Program to share their strategies for identifying and responding to customers in vulnerable circumstances, such as those experiencing financial difficulty. Encouragingly, institutions provided examples of actions relating to the protection of vulnerable customers.

Increasing staff awareness of vulnerability

Supporting staff to recognise customers who are (or are at risk of becoming) vulnerable is a priority for many institutions. This is largely achieved by training front-line staff to identify signs of financial abuse, including instances of elder abuse, financial scams and fraud, and to respond with sensitivity and compassion.

One Category A institution implemented a training program for all staff in its branches and contact centres after becoming aware that several customers – particularly elderly customers in remote areas – were showing signs of vulnerability and financial abuse.

A Category D institution provided its staff with training in how to recognise customers who may be experiencing elder abuse. This was supported by regular manager meetings to workshop examples of elder abuse and discuss possible 'red flags' for front-line staff to look out for when dealing with customers. According to the institution, this has resulted in improved outcomes for its members.

Advocating for vulnerable customers

*One Category A institution has appointed a **Vulnerable Customer Advocate** – a dedicated member of staff responsible for looking after vulnerable customers, including those who are victims of elder abuse.*

While the Vulnerable Customer Advocate is a front-line staff member, they also work with other relevant departments to ensure vulnerable customers are provided with help and support across the business.

Leveraging technology to protect vulnerable customers

In response to the increasing number of scammers and fraudsters preying on vulnerable members of the community, some Code subscribers are investing in fraud prevention technology that monitors customer transactions for unusual activity and stops suspicious transactions from proceeding. One Category A Code subscriber leveraging this technology has

[13] Refer to Appendix L: Compliance monitoring activities of the 2019–20 Annual Report.

also implemented a fraud awareness-raising program for staff and customers, which it rolls out via blogs and newsletter articles.

Empowering vulnerable customers

One Category B institution has developed a Customer Service Charter that commits its staff to protecting vulnerable customers, including those experiencing financial abuse and family violence.

The Charter is published on the institution’s website alongside the Code’s 10 Key Promises and includes information and contact details for a range of support services for people in need.

Powers of Attorney - identifying misuse

Several Code subscribers identified instances of vulnerable customers experiencing financial abuse after being coerced into giving another person (often a relative) Enduring Power of Attorney over their financial affairs.

To protect vulnerable customers from misuse of an Enduring Power of Attorney, these Code subscribers have introduced a suite of measures, including documented policies and procedures to help staff manage Powers of Attorney; and training programs to help staff recognise the signs of financial abuse, particularly towards elderly customers by their relatives where the customer has signed a Power of Attorney.

Recommendations

All Code subscribers should prioritise the protection and treatment of vulnerable customers. Some institutions shared examples of practice demonstrating that they understand the importance of staff being able to identify customers experiencing, or at risk of, financial abuse and are putting in place strategies to protect and help them.

Code subscribers are encouraged to keep exploring ways to improve protections for vulnerable customers, and to consider implementing some of the examples mentioned here.

For our part, the Committee will continue to monitor the way Code subscribers deal with vulnerable customers, with further investigation to be carried out as part of the 2020-21 ACS data collection and verification program.

COVID-19 impact

The COVID-19 pandemic presented the customer owned banking sector with significant and unexpected operational challenges during 2020. In our discussions with Code subscribers, we sought to find out to what extent their businesses were impacted by the pandemic, how they responded and what measures they had in place to assist their customers.

Business impact

The biggest impact to business was the number of customers requesting loan deferral arrangements. This put pressure on institutions' customer service, sales and financial hardship teams and resulted in the need to redeploy staff from other areas of the business to assist with customer queries.

In most cases, customers who requested a loan deferral did so in the early stages of the pandemic as a preventative measure (i.e. in the event that they found themselves in financial difficulty at some point in the future), rather than because they needed financial assistance at the time of the request.

Code subscribers were able to tell the Committee exactly how many customers had asked for COVID-19 loan deferrals, as well as the number who remain on these arrangements. All institutions reported that the majority of their customers have now recommenced their loan repayments.

How institutions responded to COVID-19

Code subscribers' responses to the pandemic focused on business continuity in two key areas: redeploying staff and assisting customers.

Redeploying staff

Having experienced a sharp spike in customer enquiries from the onset of the pandemic, many Code subscribers – particularly Category A institutions – responded by making adjustments to their workforce. Staff from areas where there was less demand (for example, Business Development) were redeployed into areas with high customer contact, such as Customer Care and Financial Hardship, to assist with the increased number of requests for loan deferrals and other customer enquiries.

One Category A institution set up a new department specifically to assist its customers during the pandemic. The department responded to each individual customer, creating a tailored approach to their specific requirements. In a similar vein, one Category B institution appointed two staff members to work exclusively with each customer that requested a loan repayment deferral.

Assisting customers

Ensuring that customers were informed and supported throughout the pandemic was a key priority for all Code subscribers.

Several institutions deployed technology to stay in touch with their customers and inform them about changes to products and services. Websites were updated to include FAQs and information about accessing assistance and forms online, and some institutions developed apps to help customers access services remotely.

Although not affected by closures due to its rural location, one Category D Code subscriber nonetheless allowed customers who preferred not to visit a branch in person to provide account instruction remotely. The same Code subscriber also took steps to identify and support customers who had no digital presence to access their accounts remotely via internet banking and by using debit cards instead of passbooks.

Many Code subscribers took a personalised approach to supporting their customers throughout the pandemic. Institutions of all sizes reported contacting customers or members individually to discuss their specific needs.

One Category B institution implemented a call-out program in response to COVID-19 that saw staff proactively telephone vulnerable customers to offer support. Staff at the same institution also visited elderly customers to discuss their needs and offer assistance.

One Category A institution established a dedicated hotline for healthcare workers to support them during the pandemic. Another Category A Code subscriber, having noted that several customers were withdrawing large amounts of cash during the early stages of the pandemic, met with these customers to determine why and provide assistance where needed.

Cool in a crisis

A few weeks prior to the pandemic hitting, one Category B institution conducted a "crisis scenario" exercise to test its procedures, prepare its staff and understand areas of risk to the business in the event of an unforeseen disruption.

The exercise enabled the institution to improve its crisis response strategy in time for the initial lockdown, and its workforce was well prepared to move quickly to a work-from-home arrangement. The institution also recognised the need to give customers a choice in how they continued to do their banking and being regionally located, chose to keep all its branches open.

Recommendations

The Committee saw examples of customer owned banks engaging well with its members during the COVID-19 pandemic.

The Committee encourages all subscribers to provide an appropriate level of support and commitment in their day-to-day operations, even as Australia recovers from the economic and social impacts of COVID-19. Institutions should review the interim measures they employed in response to the pandemic – including different ways of working for staff, new technologies and personalised approaches to meeting customer needs – and consider implementing them permanently.

Conclusion

The ACS Verification Program is a vital component of the Committee's monitoring activities. It allows us to validate and interpret the data we receive from Code subscribers, and to have meaningful discussions about what they are doing well and areas for improvement. Importantly, the Program also provides us – and subscribers – with insight into where the industry sits in terms of breach reporting, Code compliance and best practice.

Overall, subscribers have demonstrated a positive approach to their compliance monitoring and breach data reporting for the 2019–20 reporting period. As this report indicates, some institutions need to examine their monitoring and reporting culture and processes to ensure they are identifying and capturing all Code breaches, while others should closely review how they interpret specific Code obligations to ensure they match the Committee's expectations.

The data and information contained in this report provides valuable insights into emerging issues on risk and compliance, along with recommendations from the Committee and examples of better practice from some of the institutions that participated in the 2019–20 ACS Verification Program. We expect all Code-subscribing customer owned banking institutions to consider implementing the recommendations and examples for their organisation.

Appendix 1: Participating Code institutions

Table 1: Number of participating Code institutions by size and location of head office

Size of Code institution	*NSW*	*Qld*	*SA*	*Tas*	*Vic*	*Total*
Category A (over $2b in assets)	4	4	2		3	13
Category B (between $1b and $2b in assets)	4		1			5
Category C (between $500m and $1b in assets)	2	1		1		4
Category D (between $200m and $500m in assets)	1				1	2
Category E (under $200m in assets)	1					1
Total	**12**	**5**	**3**	**1**	**4**	**25**

Appendix 2: Areas of concern

*Table 2: A*nalysis of high volumes of self-reported Code breaches in 2019–20[14]

Service Standards	*Number of Code institutions self-reporting breaches of this Service Std.*	*Number of Code institutions who self-reported high number of breaches*
KP5 Deliver high customer service	15 25% of total Code institutions	• 3 Cat A institutions self-reported 83% (including 51% by one Cat A institution) and • 7 Code institutions self-reported 15% of total breaches of KP5.
KP8 Comply with legal & industry obligations	20 33% of total Code institutions	• 2 Cat A institutions self-reported 57% and • 4 Code institutions (3 Cat A and 1 Cat C) self-reported 25% of total breaches of KP8.
D2 product information	18 30% of total Code institutions	• 1 Cat A institution self-reported 41% 1 Cat A institution self-reported 15% of total breaches of D2.
D3 Interest rates, fees and charges	25 42% of total Code institutions	• 2 Cat A institutions self-reported 35% of total breaches of D3.
D16 Statement of accounts	13 22% of total Code institutions	• 1 Cat E institution self-reported 72% of total breaches of D16.
D6 Responsible lending practices	16 27% of total Code institutions	• 1 Cat A institution self-reported 33% and • 3 Code institutions self-reported 36% of total breaches of D6.
D23 Information privacy and security	33 55% of total Code institutions	• 1 Cat A institutions self-reported 57% of total breaches of D23. • 2 Code institutions self-reported over 100 breaches each. • 3 Code institutions self-reported over 50 breaches each. • 8 Code institutions self-reported over 10 breaches each.
D1 Advertising	13	• 1 Cat A institution self-reported 42% of total breaches of D1.

[14] As per Table 16 of the COBCCC Annual Report 2019-20, page 46.

Service Standards	*Number of Code institutions self-reporting breaches of this Service Std.*	*Number of Code institutions who self-reported high number of breaches*
	22% of total Code institutions	

Table 3: Analysis of high volumes of self-reported complaints in 2019–20[15]

Complaints	*Number of Code institutions self-reporting complaints in this area*	*Number of Code institutions who self-reported high number of complaints*
Product: Credit	46 77% of total Code institutions	• 6 Cat A institutions self-reported 77% of total complaints concerning credit, including one institution self-reporting over 1,000 and two institutions self-reporting over 500 complaints each.
Product: Deposit taking	51 85% of total Code institutions	• 4 Cat A institutions self-reported over 1,000 each, representing 70% of total complaints concerning deposit taking products. • 8 institutions self-reporting over 100 complaints each, representing 22% of total complaints concerning deposit taking products.
Product: Payment systems	47 78% of total Code institutions	• 2 Cat A institutions self-reported over 1,000 each, representing 70% of complaints concerning payment systems. • 6 institutions self-reported over 100 complaints each, representing 21% of total complaints concerning payments systems (including 1 Cat A institution representing 9% and 1 Cat E institutions representing 2%).
Issue: Advice	27 45% of total Code institutions	• 3 Cat A institutions self-reported over 100 complaints each, representing 77% of total complaints concerning advice issues.
Issue: Charges	39 65% of total Code institutions	• 4 Cat A institutions self-reported 82% of total complaints concerning charge issues, including one institutions self-reporting over 1,000 complaints. • 1 Cat D institution self-reported over 100 complaints, representing 2% of total complaints concerning charge issues.

[15] As per Table 26 of the COBCCC Annual Report 2019-20, page 67.

Complaints	*Number of Code institutions self-reporting complaints in this area*	*Number of Code institutions who self-reported high number of complaints*
Issue: Disclosure	33 55% of total Code institutions	• 3 Cat A institutions self-reported about 500 complaints each, representing 89% of total complaints concerning disclosure issues.
Issue: Financial Difficulty	30 50% of total Code institutions	• 2 Cat A institutions self-reported over 100 complaints each, representing 53% of total complaints concerning financial difficulty issues.
Issue: Decision by Code institution	36 60% of total Code institutions	• 4 Cat A institutions self-reported 83% of total complaints concerning decisions by Code institutions, including one institution self-reporting over 2,000 complaints (65%).
Issue: Instructions	35 58% of total Code institutions	• 2 Cat A institutions self-reported 76% of total complaints concerning instructions issues.
Issue: Privacy	32 53% of total Code institutions	• 2 Cat A institutions self-reported 59% of total complaints concerning privacy issues.
Issue: Service	42 70% of total Code institutions	• 2 Cat A self-reported over 1,000 complaints each, representing 54% of total complaints concerning service issues. • 8 institutions self-reported 37% of total complaints concerning service issues.
Issue: ATM Transactions	26 43% of total Code institutions	• 2 Cat A institutions self-reported 64% of total complaints concerning ATM transaction issues.
Issue: Transactions	47 78% of total Code institutions	• 5 institutions self-reported over 100 complaints each, representing 85% of total complaints concerning transaction issues.
Outcome: Other	9 15% of total Code institutions	• 1 Cat A institution advised that it does not currently capture the outcome of complaints as per definitions requested in the ACS.

Appendix 3: About the Code, the Committee and the Compliance Manager

The Code

The Customer Owned Banking Code of Practice (**the Code**) was developed by the Customer Owned Banking Association (**COBA**) and commenced operation on 1 January 2014. The Code replaces the 2010 Mutual Banking Code of Practice.

The Code was revised to accommodate changes the Australian Securities and Investments Commission (**ASIC**) made to Regulatory **Guide** 221[16] *Facilitating digital financial services disclosures* and the *e-Payments Code*. The revised Code was effective from 1 July 2016. A further update was published, effective 1 January 2018.

Through the Code, subscribing credit unions, mutual banks and mutual building societies voluntarily commit to fair and responsible customer owned banking.[17]

The Code is currently under review.[18]

The Committee

The Code Compliance Committee (**the Committee**) is an independent compliance monitoring body established under the Code and the Code Compliance Committee Charter (**the Charter**). It comprises an independent chair, a person representing the interests of the customer owned banking sector and a person representing the interests of consumers and communities.

The purpose of the Committee is to monitor compliance with the Code. To achieve this, the Committee monitors Code compliance and shares recommendations for good practice, engages with stakeholders and analysis the external financial services' environment and ensures efficient and effective Committee operations.

The Compliance Manager

The Australian Financial Complaints Authority (**AFCA**) provides Code monitoring and administration services as Compliance Manager[19] to the Committee and COBA by agreement. AFCA has appointed a dedicated team of staff (Code Team) within its office to undertake that task.

For more information about the Code, the Committee and the Compliance Manager, please visit **www.cobccc.org.au**.

Customer Owned Banking Code Compliance Committee
PO Box 14240 Melbourne VIC 8001
email: info@codecompliance.org.au
Phone: 1800 931 678 (free call - please ask for 'Code Compliance')
www.cobccc.org.au

[16] See **https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-221-facilitating-digital-financial-services-disclosures/**
[17] See **https://www.cobccc.org.au/code-of-practice/code-register/**
[18] See **https://www.customerownedbanking.asn.au/how-it-works/code-of-practice**
[19] As per Customer Owned Banking Code Compliance Committee Charter section 4.4.