CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

LEARNING BY EXAMPLE

A collection of self-reported Code breaches

November 2021

About this Report

Each self-reported Code breach is a miniature case study full of useful information and lessons. How was it detected? What caused it? How was it remediated short-term? What action was taken long-term to address wider implications and/or a potential systemic or process issues? Processes require ongoing maintenance – we hope these real-life examples help Code subscribers consider where work might be needed in organisations and which solutions might suit.

Disclaimer

The anonymised breach examples used in this report were not investigated by the Customer Owned Banking Code Compliance Committee, and their inclusion is not a comment on the adequacy of any remediation. The examples might, or might not, represent wider industry issues. While many instances were chosen randomly, some priority was given to breaches with a high financial impact or affecting the greatest number of customers. Examples also contained a high quality of information and/or demonstrated consideration, analysis and/or rectification by the customer owned banking institution.

Contents

Introduction

Every year, the independent committee that monitors the Customer Owned Banking Code of Practice (**the Code**) collects self-reported data from Code subscribers about Code breaches and complaints in the previous year.

In the 2021 Annual Compliance Statement (ACS), all 57 subscribers submitted information to the Customer Owned Banking Code Compliance Committee (**the Committee**). This data was supplemented by a verification program which included discussions with all subscribers.

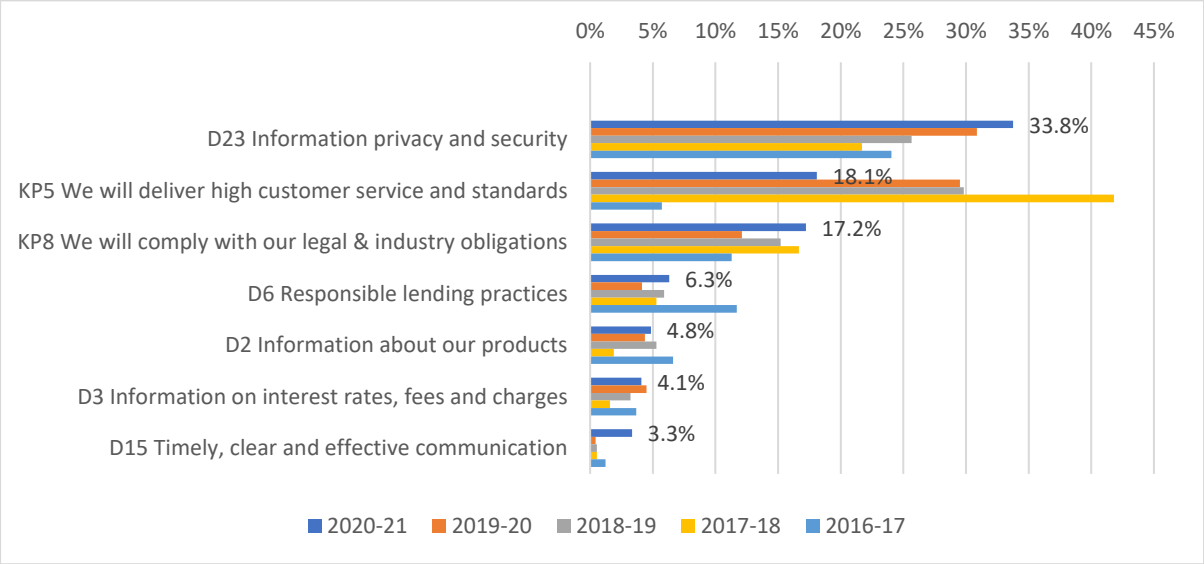
Analysis of the data helps the Committee identify industry trends and issues which it then shares with stakeholders in the Code. The findings also create a useful benchmarking tool that subscribers should use to compare the robustness of their compliance systems with the industry and other similar-sized institutions. Subscribers will have already received the Committee's Benchmark Report on the ACS findings.

The following selection of anonymised breach examples from the 2021 ACS – grouped by theme – offers insights into the many issues at play in the complex customer owned banking industry. Almost three-quarters (74%) of subscribers self-reported breaches[1], with the main areas of breach being:

- information privacy and security (one-third of total breaches) – Section D23 of the Code
- poor customer service and standards (one in five) – Key Promise 5 of the Code
- non-compliance with legal and industry obligations (one in six) – Key Promise 8 of the Code.

Responsible lending practices (Section D6), and provision of information about products (Section D2), interest rates, fees and charges (Section D3), remained an issue, while communication (Section D15) appears to have emerged as a new concern.

Chart 1: Top self-reported Code breaches over past five years.



[1] 26% of Code subscribers self-reported nil breaches in 2020-21.

The Committee was disappointed that one-quarter of self-reported breaches did not specify a particular immediate remedial action and about three-quarters did not specify any long-term remedial action.

The ACS process is designed to help subscribers learn from breaches and prevent reoccurrence. We urge subscribers to consider whether their own organisations have the appropriate processes in place including meaningful and effective short-term and long-term remedial action, as well as using the breach and complaints data to provide staff training and guidance.

Privacy

D23 Information privacy and security

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

- In one instance, detected by internal monitoring, 60 customers were affected by a combination of failure to redact Tax File Numbers (TFNs) which was then accidentally provided to unintended recipients. Training was provided. The cases were assessed, but none merited reporting to Office of the Australian Information Commissioner (OAIC).
- An internal review identified a system error related to how online banking opt-outs were fed through to marketing campaigns. An estimated 4,800 members who had opted out of marketing received between one and 12 marketing messages, with an average of five, mostly in a 12-month period. Online banking opt-outs are now excluded from marketing campaigns and further analysis was done on marketing opt-out codes.
- It was discovered in an internal review that a third party was storing bank data, including member data of about 6,500 customers, in North America although it had indicated it would be stored in Australia. A review was completed and migration of the data to Australia was finalised.
- Five hundred customers were affected by a system error related to online banking passwords. When prompted to change their passwords, members input their choice into a free text box, however the password was being captured in the Event details on their membership. The campaign was pulled, and testing done to see if the fields could be locked down. The customer owned bank reviewed their Events system and communication with customers.
- An internal audit revealed that in 12 instances, staff making outbound calls failed to state that the call would be recorded. A 13th breach was identified by the contact centre team leader during a monthly audit. The contact centre team received communications about privacy requirements and protocols for outbound calls and the compliance manager conducted a privacy training session with the team.
- A monitoring program found that a call recording system had continued to record when customers were transferred to an associated third party. The system was altered to disable recording once a call had been transferred externally and the recordings of 785 transferred calls were being deleted.

- A member was tricked into supplying information to a fraudster. The fraudster made four calls to the customer owned bank over two days, with three of the four failing the customer owned bank's authentication processes. Based on the circumstances of this incident, the staff member was terminated and $27,750 was reimbursed to the member. The incident led to improvements in the authentication process and regular training for staff. OAIC was notified.

KP8 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.

- An audit of returned mail/email/failed text messages found that 13,000 members did not have valid addresses. Privacy principles require institutions to take reasonable steps to update personal identifiers where it is known information is out of date or incorrect. Analysis of member communications was done, and controls used to notify members that information is incorrect were explored. Staff training will ensure information is updated during member interactions.
- A compliance review found that some dormant memberships had not been actioned, e.g. the membership accounts had not been accessed for some time and no contact had been made. As a result, 27 memberships were not reported to the Australian Securities and Investments Commission (ASIC) as unclaimed. Investigations found that staff were not actioning dormant members as a priority and could not determine when a member had been added to the dormancy database. The dormancy system will be reviewed and updated; processes will be updated to ensure staff understand dormancy and unclaimed money requirements. The memberships in the dormancy system are being reviewed.
- At a micro institution (up to $200m in assets), 42 International Fund Transfer Instruction (IFTI) reports had not been submitted to AUSTRAC. Staff thought that only transactions over $10,000 needed to be reported, not every IFTI transaction. The reports were lodged, and the issue attributed to insufficient training and lack of understanding of the reporting obligations. Procedure has been reviewed.
- A staff member realised that a required Employee Due Diligence screening for new employees commencing in high risk roles had not been done for 12 months. The employees were screened, and processes changed to prevent reoccurrence.

General service standards

KP1 We will be fair and ethical in our dealings with you

We will always act honestly and with integrity and will treat you fairly and reasonably in all our dealings with you.

- A customer owned bank received a complaint from a trans woman who had visited a branch. A cashier, when phoning another employee for help with the customer's matter, had twice referred to the customer as "he", despite the customer being legally female, her customer owned bank profile reflecting this, her using the title "Miss" and wearing female clothes. The customer suggested staff may need training in how to deal with trans people and should rely on the preferred title in the system to ensure

they get it right. The customer received an apology. A note was added to her profile for phone inquiries to advise of her status.

KP2 We will focus on our members

We will place a high priority on service, competitiveness and customer focus. We will provide friendly and reliable service to our customers. Our customer service standards will be appropriately tailored where we are aware that you have special needs (for example, because of your age or a disability, because you are an indigenous person, because English is not your first language, or because you are unfamiliar with financial products and services).

- A NSW customer had paid for a "greenslip" (compulsory third-party car insurance cover) at their customer owned bank, but later found their car registration had not been renewed because the payment had not gone through. The customer owned bank determined that, because the customer was a pensioner and not required to pay car registration, the customer owned bank's greenslip error had not been detected. The customer owned bank amended its procedures to address this.

KP5 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.

- A migration to new IT infrastructure caused a week-long outage for a customer owned bank's internet banking and native apps, resulting in many members being unable to access services or experiencing extreme delays. Due to the significant nature of the breach, it was referred for external legal advice. While not obliged to inform ASIC, a voluntary notification was made to APRA. During the outage, many departments worked together to assist members, including offering extended hours and offering regular notifications on its website and social media. A series of remedial and preventive actions were implemented in response to the incident.

Disclosure, information and communication

KP3 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.

- A branch of a customer owned bank spotted incorrect and outdated inclusions on flyers for a new insurance campaign. The flyers were recalled and destroyed. A graphic designer had used an outdated working file. The customer owned bank determined that the root cause of this error was that its system's functionality prohibited design files from being saved appropriately when designers worked remotely. The process is currently being reviewed.

- When a member decided to refinance a loan, the member found that at the loan's inception, a staff member had failed to say that some product features would be lost if varying the loan to a standard product. In remediation, the customer owned bank paid an interest adjustment of $8,696 over the six-year period.

D2 Information about our products

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

- An internal review found that a Key Fact Sheet (KFS) was not available for a special offer on a two-year fixed rate product – when a product is offered online, a KFS must also be available online. The product was removed from the website and a KFS deployed for issuance if requested via other channels. The product checklist was enhanced to capture this requirement in the future.

D3 Information on interest rates, fees and charges

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.

- A sentence disclosing that additional costs may apply to fixed rate home loans was omitted from the newest version of the home loan disclaimer on the website, impacting 146 customers who had a fixed rate home loan approved and funded while the incorrect disclaimer was live. None of the customers had been charged a prepayment fee in this period. The disclaimer was added to the website.
- An employee noticed that business account flyers were inconsistent with new Terms and Conditions (T&Cs), that they included old fees that were not charged anymore and that fee changes had not been updated. A review of the flyers and product schedules was undertaken to align the content with current T&Cs and fees.
- When a long-term customer changed home loan packages, he says he was not informed that, under the new loan terms, he would now have to pay transaction fees on an everyday account if his transactions exceeded 20 per month. He had not paid fees in his previous 30 years with the customer owned bank. The customer owned bank reimbursed fees totaling $878.

Communication

D15 Timely, clear and effective communication

We are committed to timely communication with our customers.

- For five months, all online 'Pause your repayments' application forms were sent to an unattended email inbox. Of the 43 applications made in this period, three customers waited more than 45 days for a response. The cause was determined to be a system issue compounded by a lack of ownership of the process. All applications were actioned, and the system issue fixed.
- Two members of a customer owned bank were approved for a joint construction loan, which factored in a $25,000 building grant the Home Finance Manager mistakenly said they were eligible for. After settlement, the grant was rejected, and the members

were $25,000 short of the amount needed to finalise construction. Investigation of the members' complaint resulted in an ex gratia payment of $25,000 by the customer owned bank towards the loan. The staff member was disciplined and given further training.

D16 Account statements and balances

We will provide you with regular account statements clearly setting out all transactions relating to your deposit and loan accounts with us.

- An internal review identified a gap in process where members releasing funds, or closing term deposits early, were not provided with a statement or formal notice outlining the early release fee, although it appeared in the original T&Cs. This occurred 19,634 times over six years. ASIC was notified, the system has been corrected to disclose the fee automatically and the customer owned bank will undertake a compliance review of all term deposit processes.
- After two member complaints and an internal review of deposit products, a customer owned bank identified potentially 3,000 non-individual members (companies, trusts, superannuation funds, etc) who may have missed statements because they had elected to receive them electronically but could not access them through online banking. A data fix removed the eStatement method of delivery for non-individual memberships. The customer owned bank is reviewing the statement process and mapping the system rules for statements. Exception reports are also being developed to identify statement issues.

Responsible lending

KP4 We will be responsible lenders

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

- One customer owned bank self-reported a number of separate breaches of this standard involving members with overdrawn accounts being allowed to open new accounts, leading to multiple overdrawn and inactive accounts that required debt recovery. The breaches occurred due to manual error. Staff were provided with additional training.
- A loan was assessed and approved, however the lender failed to include additional debt held by the customer's business. The loan is being reassessed and modified to reflect the applicant's full financial position. The customer owned bank is currently reviewing the matter as to whether to reimburse any costs associated with a declined loan.

D6 Responsible lending practices

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

- An audit undertaken by one customer owned bank revealed a number of breaches of this obligation involving staff members failing to obtain or verify all of the information required to assess a loan approval accurately. These included: not capturing or including expenses; failing to obtain or verify current proof of income; and, declaration questions not being verified. A review of process and procedures and further staff training was undertaken.

- Failure to follow process led to a loan being approved for a customer severely impacted by financial hardship and family violence. Had she tried to comply with the loan's obligations, her long-term financial situation would have become dire. A complaint about irresponsible lending led to a full debt waiver and credit inquiry listing being removed. The Committee is currently undertaking an own motion inquiry into this area.

Advertising, terms and conditions

D1 Advertising

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 compliance review found that after a website launch, some page elements did not display correctly in Internet Explorer, resulting in missing disclaimers, disclosures and rate information. It was attributed to a blend of human and system error, with the implications of such an error not being understood by the website's creators and it not having been tested appropriately as a result. Pop-up messages were added within Internet Explorer to confirm that it was not compatible with the website; when clicked, they opened a different browser.
- Out-of-date brochures containing incorrect information about fee-free transactions were discovered in three branches in an internal review. It is unclear how many members, if any, would have been given these brochures. The brochures were recalled and controls regarding sales literature were tightened.
- More than 3,200 people visited a website that incorrectly displayed an interest rate as being 'from 2%', when it should have read 'from 1%'. A staff member noticed the error. The site was corrected, and processes reviewed and amended. Compliance staff are now also required to check the website when changes to products such as rates or fees occur.

D4 Fair terms and conditions

The standard Terms and Conditions applying to our products and facilities will be:
- clear, unambiguous, and not misleading
- distinct from our advertising and promotional material
- written in a plain language style, and legibly presented

- T&Cs for an everyday account did not make it clear that a bonus interest feature on external transfers would apply to salary payments only. A member complaint led to the identification of 407 instances where bonus interest hadn't been paid, affecting 214 members. Interest totaling $19,917 was paid in remediation and the T&Cs were clarified and communicated to members. The matter was reported to ASIC.
- A deposit account campaign on Facebook intended for specific recipients was shared by them, which led to others requesting payment of advertised cash payments. One complaint led to an ex-gratia payment of $75. The Facebook campaign's T&C's were updated and approved by the legal department.

D5 Reviewing fees and charges

We will regularly review any fees and charges on our products and services, including their level.

- Auditors discovered that following a fee structure update, a fee previously classified as a service fee became a transaction fee, which was then erroneously applied to transaction-fee free accounts held by 571 members. The fees were reimbursed, and a communications plan implemented. Long-term remediation included considering fees fully when updating products and services and an ongoing review of fees and charges applied to accounts.
- A system workaround that waived a $10 fee for card replacement (because the fee was not included in the customer owned bank's fees and charges schedule) was not being followed, affecting 121 members. The fees were reimbursed, and a system fix has been established to prevent the fees from being charged in the future.

Complaints resolution

D27 Prompt, fair resolution of complaints

We have an internal process for handling complaints of our customers in relation to the products and facilities we issue.

- Monitoring identified that a customer complaint about a loan being declined had been closed after a lengthy conversation, but without a letter being sent that outlined internal and external dispute resolution options. The member received an apology and the letter.
- A customer whose account was frozen complained to the Australian Financial Complaints Authority (AFCA) that his customer owned bank did not respond to calls for some time, and that when he supplied the ID necessary to unfreeze the account, the customer owned bank did not act on this and he remained unable to access funds. The issue, attributed to staffing issues, was resolved with an apology and an explanation that recent increases in identity theft via a particular channel had caused the initial issue.

About the Code

The **Code** sets standards of good industry practice for the 57 Code subscribers[2] that have agreed to comply with its provisions when dealing with current and prospective individual and small business customers. By subscribing to the Code, customer owned banking Code subscribers have voluntarily committed to uphold good industry practice, promote informed decision-making about their services, and act fairly and reasonably in delivering those services.

The Code is owned and published by the Customer Owned Banking Association (**COBA)** – the industry advocate for Australia's customer owned banking sector – and forms an important part of the broader national consumer protection framework and financial services regulatory system.

The Code was revised on 1 July 2016 to accommodate changes made by **ASIC** to **Regulatory Guide 221** *Facilitating digital financial services disclosures* and the *e-Payments Code*. A further update was published, effective 1 January 2018.

The Code is currently under review.

About the Committee

The Committee is an independent compliance monitoring body established under the Code and the Code Compliance Committee Charter **(the Charter**). It comprises of three members: an independent Chair, an Industry Representative and a Consumer Representative. The Code and Charter entrusts the Committee with several functions and responsibilities.

The Committee monitors compliance with the Code, identifies systemic industry-wide issues and promotes good industry practice.

About the Compliance Manager

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

Definitions

For ease of reference when reading this report:

- 'the Code' means the 2018 Code unless otherwise stated.
- 'customers' include individuals or small businesses that are current and prospective customers of Code subscribers.
- 'Code subscribers' means customer owned banking institutions that subscribe to the Code.

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

[2] Number of Code subscribers as at 30 June 2021