CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

Managing privacy compliance

Lessons from the 2017 Annual Compliance Statement Verification Program, Part 1

18 May 2018

Introduction

Each year, the Customer Owned Banking Code Compliance Committee holds in-depth compliance discussions with a sample of institutions for the Annual Compliance Statement Verification Program. This gives the Committee valuable insights into institutions' day-to-day management of their Code compliance obligations. These insights can inform best practice for institutions and improvements to the Committee's own compliance monitoring activities.

Collecting the data

In November and December 2017, Committee staff held individual teleconferences with compliance staff from participating institutions. In each discussion, the Committee sought more information about:

- how the institution **manages and monitors Code compliance**
- any information **privacy breaches** it had reported in the Annual Compliance Statement
- the institution's **compliance culture, and any good practices** employed.

In preparation for the discussion, each institution was given a copy of its 2016–17 ACS response as well as a benchmarking report that presented its compliance data alongside information about other institutions of a similar size and industry performance overall.

Most participants welcomed this 'like for like' comparison and insight into industry trends. However, some institutions said that variation in how institutions record and report complaints makes accurate comparisons difficult.

Participating institutions

Twenty-four institutions participated in the ACS Verification Program, including:

- **all** large institutions (over $1b assets)
- **all** institutions that reported a privacy breach in their 2016–17 ACS
- **a sample** of micro, small and medium institutions.

Participants were geographically spread and varied in size.

Other papers in this series

For more insights from the ACS Verification Program, see the two other papers in this series:

- *Better breach reporting*
- *Better complaint reporting*

Privacy

The privacy provisions in section D23 of the Code were a focus of this year's ACS Verification Program. All 22 Code subscribers that had reported a breach of these obligations in the ACS participated, providing more information about these breaches and any related complaints. This gave the Committee new insights into how institutions manage this vital area of compliance.

Minimising breaches from human error

Participants reported that most privacy breaches are the result of isolated human error or an individual's failure to follow established procedures. Commonly, breaches involved customer's personal and account information – such as account statements, letters and lending documents – being mistakenly provided to an unauthorised party at a branch, by mail, email or secure email.

Participants reported breaches where non-signatories to an account, such as partners or parents, were able to access account information, make withdrawals or cancel payments. Staff failures to update or remove a signatory from previously joint accounts also led to breaches.

A number of privacy breaches concerned consumer credit files. For example, credit files were accessed without the necessary authorisation; credit checks were processed with incorrect customer information; and tax file numbers were not removed or redacted from customer applications. One participant also reported a breach involving the retention of superannuation statements for longer than necessary.

These breaches demonstrate that while compliant systems, policies and procedures are vital, they are insufficient. The fact that most reported privacy breaches were caused by human error and deviation from procedure highlights the critical importance of ongoing and refresher training, as well as routine alerts and reminders for staff.

> Good practice example

Actively engaging staff in training

One micro institution learned that although staff signed a confirmation statement after completing training, they weren't very engaged with the training. To encourage more active engagement, the institution created a follow-up 10-question quiz with questions that are reviewed and updated annually. The institution reports that this tool has helped staff to engage more in the training and remember what they have learned.

Managing risk from systems errors

While most privacy breaches reflected human error, systems errors also contributed. In one example, multiple customer statements were uploaded to the incorrect account due to a systems error.

Transfers or upgrades to banking platforms can create the circumstances for privacy breaches. At one institution, customers were temporarily able access other customers' statements, while at another, increased call volumes following a system upgrade lead to incorrect data entry. Regular systems checks and testing are essential.

Identifying privacy breaches

Most information and privacy breaches were identified when the incorrect recipient of the information contacted the institution, or when the staff member who made the error self-reported it. This high level of self-reporting is a pleasing sign of increasing awareness of privacy obligations. Participants also reported identifying breaches through targeted retrospective or hindsight reviews, for example, of lending files.

In light of the number of 'wrong letter, wrong envelope' situations, most of which were identified by the incorrect third party recipient contacting the institution, it is likely that many of these breaches still go undetected. Once a breach is reported, institutions should immediately assess whether other clients are affected and inform them accordingly. To maintain client trust, this advice should include information about how the breach was rectified.

Responding to breaches

Institutions generally responded to identified privacy breaches by:

- asking the incorrect recipient to confirm that the information was destroyed
- telling the impacted customer about the breach and offering an apology and/or another goodwill gesture, such as a refund
- providing remedial training, coaching, feedback and staff training or refresher courses.

Privacy breaches are also discussed in staff meetings and as knowledge-sharing exercises. Repeated or common errors by a wider group of staff can also lead to a review of procedures.

> Good practice example

Reaching more staff with compliance monitoring

One large institution conducted a compliance monitoring exercise in which a case study or scenario would be read out over the phone, followed by questions testing the staff member's knowledge of compliance issues. Staff were selected for telephone surveys based on key risk areas, previous breaches or other data, and the exercise reached three or four people each month.

Recently, the institution expanded this monitoring exercise with email quizzes. Some quizzes are mandatory, while others are voluntary – but there are incentives to participate. With this approach, the compliance team reached a larger and more diverse group, engaging around 200 staff.