CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

Better breach reporting

Lessons from the 2017 Annual Compliance Statement Verification Program, Part 2

25 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:

- *Managing privacy compliance*
- *Better complaint reporting*

Breach reporting

Many Code subscribers can do more to identify, record and report breaches by making better use of complaint data and considering a wider range of breach data sources.

Making better use of complaints to identify breaches

Most participating institutions continue to rely on complaint and incident registers as the main source of Code breach data. Although most institutions reported that the Code is a consideration when reviewing complaints, a small number said that generally, they do not actively consider the Code during this process.

Code subscribers can do more to identify where complaints relate to Code breaches in complaints. Almost half the participating institutions reported zero Code breaches from complaints received – even where complaint volumes were high. For example, one large institution reported 3,072 complaints but no Code breaches.

Even when institutions have reported Code breaches – and even for institutions that use a complaints register as the sole source of breach data – the breach numbers are much lower than the Committee would expect. For example, another large institution reported 16 Code breaches from 4,960 complaints received.

> Good practice example

Flagging potential Code breaches

When logging a complaint, it is now mandatory for staff at one large institution to consider whether the complaint has a potential regulatory impact using a scale of likelihood. If something is flagged with a regulatory impact, the legal and compliance team assesses whether the incident involves a Code breach. The institution now also has a dedicated data analyst in its consumer advocacy team to analyse the complaints and breach data.

Considering all potential sources of breach data

Most participating institutions continue to rely on complaint and incident registers as the main – and sometimes only – source of Code breach data.

However, some institutions also identify Code breaches through:

- **audits**, including targeted internal audits (e.g. responsible lending); spot check audits by managers; and internal and external audits
- **reviews** of policies, procedures and products
- **monitoring and quality assurance**
- **third party feedback**.

All institutions should consider all potential sources of breach data, rather than relying too heavily or even exclusively on complaint registers.

Positively, many organisations have instituted a formalised process for internal referrals, providing a form for staff to report potential Code breaches. Accordingly, the number of breaches identified through internal staff referrals has been increasing.

Institutions need to analyse complaints data in order to rectify issues including breaches of the Code.

This demonstrates the value of efforts to create a culture and framework that supports breach and complaint reporting. Staff training and communication are vital.

> Good practice example

Improving the incident management system

One large institution implemented a new incident management system. All incidents – not only those related to licence and regulatory obligations – are assessed against the ten key promises and the provisions of the Code. In the year following implementation, this change led to a large increase in recorded Code incidents, up from 100 to 300.