CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

ANNUAL REPORT

2015–16

Analysis of self-reported breach and complaints data regarding the Customer Owned Banking Code of Practice and report on the compliance work undertaken by the Customer Owned Banking Code Compliance Committee during the 2015-16 period.

December 2016

Contents

About this report

This report assesses customer owned banking institutions' compliance with the 2014 Customer Owned Banking Code of Practice by analysing aggregated industry data for the period 1 July 2015 to 30 June 2016.

Data has been collated from monitoring the activities of the 73 institutions that subscribed to the Code in 2015–16, and consists of the outcomes of the 2016 Annual Compliance Statement and Verification Program, and investigations into alleged Code breaches.

This report also reviews the Customer Owned Banking Code Compliance Committee's monitoring activities from 1 July 2015 to 30 June 2016, and shares examples of good industry practice – as well as the initiatives of Code Subscribers – to improve standards of practice and service in the Australian customer owned banking industry.

Foreword

A focus on customers is built into the structure of customer owned banking institutions, setting them apart from other financial services providers. Customer owned banking institutions are ideally and uniquely placed to lead the sector in customer service standards. In this task, the Customer Owned Banking Code of Practice is a valuable tool. The goal of the independent Committee responsible for monitoring compliance with the Code in 2015–16 was to assist Code Subscribers to establish, maintain and share good practice for the benefit of customers, institutions and the industry as a whole.

The year brought challenges for the customer owned banking industry as regulation and compliance obligations evolved. Against this backdrop, the number of breaches and significant breaches reported by Code Subscribers increased. The Committee believes that rather than indicating poorer standards, this is likely to be an indication that institutions are embracing positive breach reporting in both their frameworks and cultures, meaning that problems are resolved at an early stage and systemic issues are found and addressed.

Many of the breaches reported in 2015–16 concerned the Code's privacy provisions. This non-compliance was not reflected in related complaints, perhaps suggesting that customer detriment was contained. Nevertheless, the Committee noted the growth in self-reported privacy breaches and encourages Code Subscribers to review and strengthen their compliance processes in this area.

Another development in 2015–16 was the decrease in complaints handled through institutions' internal dispute resolution (IDR) processes. As this appears to have coincided with a growing focus on analysing and acting on customer concerns and feedback, we are hopeful that the trend may reflect earlier detection and rectification of breaches, which minimises customer impact and the number of resulting complaints.

This year the Committee continued to work closely with the Customer Owned Banking Association (COBA), engaging productively with industry through COBA's successful compliance forums, and sharing information through regular meetings. The Committee would like to thank COBA for its support of our activities. The work of the Code Team, under the leadership of Sally Davis, has also been integral to our success. The Committee thanks the General Manager, Sally Davis, the Compliance Manager, Daniela Kirchlinde, and their staff for their careful and dedicated work.

Sue-Anne Wallace

Dr Sue-Anne Wallace
Chairperson
Customer Owned Banking
Code Compliance Committee

Sally Davis

Sally Davis
General Manager
Code Compliance & Monitoring
Financial Ombudsman Service
Australia

Year at a glance

73

customer owned banking institutions subscribed to the Code

▼ in comparison to 80 in the previous year.

11

significant Code breaches were self-reported by 7 Code Subscribers (page 14)

▲ in comparison to 5 significant Code breaches self-reported by 5 Code Subscribers in the previous year

68%

of institutions self-reported Code breaches

▲ **7%**

from the previous year (page 10)

818

Code breaches were self-reported by institutions

▲ **27%**

from the previous year (page 10)

30%

of self-reported Code breaches related to privacy obligations (page 12)

▲ in comparison to 20% in the previous year

14,100

self-reported complaints handled by their internal dispute resolution process

▼ **16%**

from the previous year (page 16)

93%

of self-reported complaints were resolved within 21 days or less

31%

of self-reported complaints related to service (page 18)
▲ from 18% in the previous year

20%

of self-reported complaints related to charges (page 19)
▼ from 29% in the previous year

Investigated three alleged Code breaches

See page 27 ➔

Analysed 73 Annual Compliance Statements

See page 10 ➔

Conducted 12 individual compliance verification audits

See page 24 ➔

Gave four presentations on Code issues as part of the COBA Compliance Forum

See page 30 ➔

Attended six industry and consumer conferences, including two presentations

See page 30 ➔

Engaged with consumer advocates, ASIC, FOS and CIO at regular stakeholder meetings

See page 30 ➔

Hosted a consumer advocate luncheon

See page 30 ➔

Issued 11 publications

See page 31 ➔

About the Code

The 2014 Customer Owned Banking Code of Practice sets standards of good industry practice for the institutions that have agreed to comply with its provisions when dealing with current and prospective individual and small business customers.

The Code has recently been revised to accommodate changes the Australian Securities and Investments Commission (ASIC) made to Regulatory Guide 221 *Facilitating digital financial services disclosures* and the *e-Payments Code*. The revised Code has been effective from 1 July 2016.

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.

KEY PROMISES

The Code sets out Code Subscribers' commitment to comply with the Code's obligations, and explains the Code's relation to laws and regulations. The Code includes:

- 10 key promises containing general principles or values that apply to all customers, as well as the broader community
- 30 specific sections detailing how these key promises are to be delivered by Code Subscribers, and
- information on how the Code is administered.

Code Subscribers have committed to the Code's 10 key promises, which apply to all customer owned banking services delivered by Code Subscribers to individuals and small business across Australia.

Table 1: The 10 key promises

1.	We will be fair and ethical in our dealings with you.
2.	We will focus on our customers.
3.	We will give you clear information about our products and services.
4.	We will be responsible lenders.
5.	We will deliver high customer service and standards.
6.	We will deal fairly with any complaints.
7.	We will recognise our customers' rights as owners.
8.	We will comply with our legal and industry obligations.
9.	We will recognise our impact on the wider community.
10.	We will support and promote the Customer Owned Banking Code of Practice.

By subscribing to the Code, customer owned banking institutions have voluntarily committed to uphold good industry practice, promote informed decision-making about their services, and act fairly and reasonably in delivering those services. Code Subscribers as at 30 June 2016 are listed in **Appendix A**.

CODE COMPLIANCE COMMITTEE

The Code Compliance Committee (the Committee) is an independent compliance monitoring body established under Section 4 of the *Customer Owned Banking Code Compliance Committee Charter* and Part E of the Code under the authority of the Board of COBA.

The Committee is assisted in its work by the Financial Ombudsman Service (FOS) Australia (the Code Team), which provides Code monitoring and administration services to the Committee and COBA by agreement.

Vision and principles

The Committee's vision is to promote compliance with the Code and to help Code Subscribers meet the Code's standards of good industry practice. The Committee supports the Code's principles and commitments by promoting the Code's benefits and seeking to influence positive changes in industry behaviour. The Committee's work is based on four key principles:

Table 2: Committee principles

1. **Independence** in its operations, governance and decision-making
2. Accountability in undertaking its functions for the benefit of the customer owned banking sector and its customers
3. **Transparency** through open engagement with stakeholders
4. Fairness in its deliberations and processes

Functions

The Committee has three main compliance and monitoring functions:

- monitoring compliance with Code obligations, including conducting Own Motion Inquiries
- investigating complaints made by any person or as a referral that a Code Subscriber has breached the Code, and
- engaging with stakeholders about Code compliance and advising on Code matters and Committee operations.

This approach allows the Committee to be strategic in assisting the industry to identify issues and emerging risks, while also dealing with individual instances of Code breaches.

In 2015–16, the Committee met formally five times; one of these meetings was held via teleconference. It also had informal individual meetings with the Code Team via telephone conferences, as well as meetings with COBA, regulators and other stakeholders. The Chairperson meets with the Chair of COBA's Board of Directors from time to time.

Committee members

Dr Sue-Anne Wallace
Chairperson
BPharm, BA (Hons), PhD,
Grad Cert Mgt, Adv Dip Arts, FAICD

Appointed: 18 February 2014[1]
Term expires: 18 February 2019[2]

Sue-Anne has extensive experience in the not-for-profit sector. Now in her fourth year as independent chair of Customer Owned Banking Code Compliance Committee, she is also Vice-President of the international certifier Humanitarian Quality Assurance Initiative (Geneva). She was formerly chair of the Australian Council for International Development's Code of Conduct for the past six years. She holds non-executive director positions with several other organisations.

For the past 12 years, Sue-Anne has focused on governance and self-regulation in the not-for-profit sector. In 2014 she was awarded a Churchill Fellowship to investigate self-regulatory codes of conduct and complaints handling in the not-for-profit sector.

Carolyn Bond AO
Consumer Representative

Appointed: 1 March 2015
Term expires: 28 February 2017

Carolyn has worked in the consumer advocacy field for more than 20 years, focusing primarily on issues including high-pressure selling, consumer credit, debt collection and credit reporting. Carolyn headed up specialist consumer legal centres, including the Consumer Action Law Centre, for 15 years.

Carolyn has been Chair of the Consumers' Federation of Australia, and has represented consumer interests on a number of bodies, including the Victorian Legal Services board, the Energy and Water Ombudsman (Victoria) board, the Banking and Financial Services Ombudsman board and the Commonwealth Consumer Affairs Advisory Committee.

Anita Schut
Industry Representative
BA (Asian Studies), Grad Dip Personnel Mgt

Appointed: 1 January 2014
Term expires: 31 December 2019[3]

Anita is the Compliance Manager at Maritime Mining and Power Credit Union and is the informal Chair and founder of the NSW Mutual Compliance Group. She has more than 15 years' experience working in compliance, including as Banking Compliance Manager for Citibank Australia, and extensive broader experience with the financial services industry, including roles in lending and human resources.

Anita has completed the Australian Compliance Institute Certified Compliance Professional program.

[1] Appointed under the revised Code (section 5.5). Previous term under 2010 Mutual Banking Code of Practice: 18 April 2013 to 18 April 2016.
[2] Final term, not eligible for re-appointment.
[3] Re-appointed as at 31 December 2016, final term, not eligible for re-appointment.

Code Team staff

Sally Davis
General Manager
Code Compliance & Monitoring
BComm, LLB, Grad Dip (Arts)

Appointed: Sep 2015 – current

Sally commenced as General Manager of Code Compliance and Monitoring at the Financial Ombudsman Service Australia (FOS) on 1 September 2015.

Sally previously worked as Senior Manager of Systemic Issues at FOS and has worked at FOS and its predecessor schemes for over 15 years. Sally is an accredited mediator and holds a Bachelor of Commerce and a Bachelor of Laws degree from the University of Melbourne and a Graduate Diploma (Arts) from Monash University.

Sally brings to this position extensive experience in financial services, as well as good relationships with regulators, industry and consumer groups from her work as Senior Manager of Systemic Issues and other roles at FOS.

Daniela Kirchlinde
Compliance Manager
BComm, Grad Dip (Finance and Investment)

Appointed: Oct 2009 – current

Daniela has a background in dispute resolution and broad insurance industry experience in Australia, England and Germany.

Daniela previously worked as Complaints and Compliance Manager at FOS and its predecessor schemes for over 20 years.

In addition to her Compliance Management role, she manages compliance for the Insurance Brokers Code of Practice.

Daniela holds a Bachelor of Commerce from the Cologne University (Germany) and a Graduate Diploma in Finance and Investment from the Australian Securities Institute Melbourne.

Code monitoring activities

The Committee's Code monitoring program provides customer owned banking institutions with an effective mechanism for self-assessing their Code compliance, monitoring and reporting frameworks, while providing the Committee with robust data on Code compliance by Subscribers. During the reporting period, the key Code monitoring activities were the Annual Compliance Statement (ACS) program and the ACS Verification Program. The ACS program requested Code Subscribers to self-report Code breaches and complaints for the 2015-16 period. The ACS Verification Program validated compliance issues which Code Subscribers previously reported for the 2014-15 period.

ANNUAL COMPLIANCE STATEMENT PROGRAM

The ACS is a self-assessment tool that helps Code Subscribers review their compliance with Code obligations every year. For Code Subscribers, completing the ACS is a core monitoring obligation. Collecting Code Subscribers' data via the ACS program forms part of the monitoring role of the Committee as established under section E21 of the Code.

Developing and improving the 2016 ACS

The 2016 ACS was reviewed and enhanced in partnership with COBA and a selection of Code Subscribers to achieve a consistent compliance monitoring approach. The ACS assessed:

- how effectively Code Subscribers complied with their Code obligations during the reporting year
- the robustness of their Code compliance monitoring frameworks
- how effectively Code Subscribers monitored their compliance against Code obligations
- instances of non-compliance and how they were remedied
- emerging or significant risk to Code Subscribers' compliance with Code obligations, and
- areas of good industry practice that can be shared with the sector.

In 2016, the online portal for ACS completion was also improved for easier access and record-keeping. Institutions had previously raised concerns about the portal's 'time out' period and its lack of a submission printing function; these issues were addressed and rectified for the 2016 ACS.

Self-reported Code breaches

The ACS gathers two distinct breach data sets: 'breaches' and 'significant breaches'. A **breach** is defined as a failure to comply with the obligations of the Code regarding the provision of a customer owned banking service.

In 2015–16, 818 Code breaches were self-reported by Code Subscribers, an increase of 27% (172) on the 646 breaches reported in 2014–15. Around two-thirds (68%) of Code Subscribers self-reported one or more breaches of the Code, up from 61% in the previous reporting period. Around one-third (37%) of Code Subscribers reported between one and ten Code breaches.[4] Just seven Code Subscribers collectively accounted for almost half (48% or 396) of the total of 818 Code breaches.

Most self-reported breaches were identified through quality assurance programs and internal audit processes. In addition, almost one-third (31%) of breaches were identified as a result of customer complaint investigations, down from 36% in the previous year.

To ensure that reporting accurately reflects performance, the Committee will continue to assist Code Subscribers with their compliance processes and encourage the embedding of positive breach reporting in institutions' culture and frameworks.

Types of breach

Chart 1 covers the four years from 2012–13 to 2015–16, identifying the percentage of each year's self-reported Code breaches that fell into the five broad categories of Code obligations.

Chart 1: Self-reported breaches by Code category 2013–16

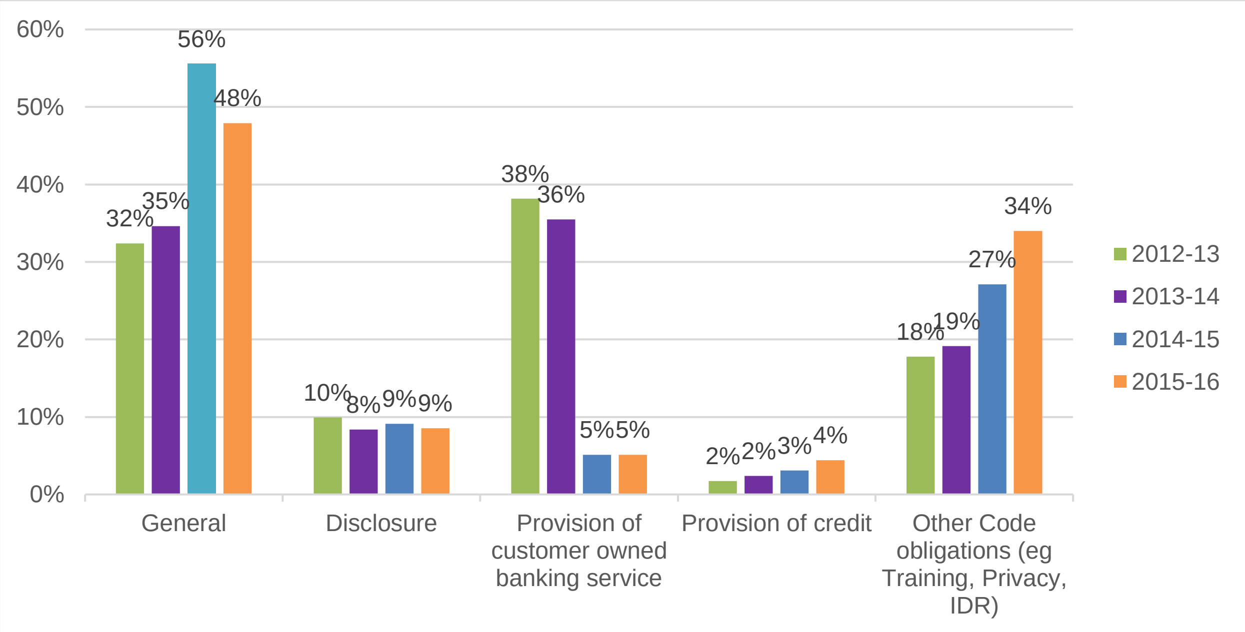


Chart 1 shows that the largest category of non-compliance in 2015–16 was 'General commitments', which comprised 48% of Code breaches. A further 34% of Code breaches were within the category of 'Other' obligations. Together, the two broad categories represented 82% of total Code breaches reported in 2015–16; very similar to the 2014–15 figure of 83%.

Table 3 provides greater detail, examining areas of non-compliance of specific Code obligations over the same four-year period.

[4] See Appendix F, table 16 on page 46.

Table 3: Self-reported breaches of Code obligations 2013–16

	2012-13	2013-14	2014-15	2015-16
General	**32.4%**	**34.6%**	**55.6%**	**47.9%**
Key commitments	**31.3%**	**32.0%**	**49.2%**	**41.3%**
KP1 We will be fair and ethical in our dealings	0.0%	0.3%	4.0%	0.4%
KP2 We will focus on our customers	4.5%	2.6%	3.1%	3.3%
KP5 We will deliver high customer service	18.1%	15.9%	25.1%	20.3%
KP7 We will recognise our customers' rights	0.0%	0.0%	0.0%	0.4%
KP8 We will comply with our legal and industry obl.	8.6%	11.1%	17.0%	15.9%
KP9 We will recognise impact on community	0.1%	2.1%	0.0%	1.1%
Provision of general information	**1.1%**	**2.6%**	**6.3%**	**6.6%**
KP3 We will give you clear information	0.0%	0.0%	0.0%	3.3%
D2 Information about our products	1.1%	2.5%	4.8%	2.8%
D19 Copies of documents, statements	0.0%	0.1%	1.5%	0.5%
Disclosure	**9.9%**	**8.4%**	**9.1%**	**8.6%**
Interest rates, fees and charges	**6.1%**	**8.1%**	**8.8%**	**6.6%**
KP3 We will give you clear information	2.9%	3.6%	5.1%	2.1%
D3 Information on interest rates, fees and charges	2.5%	4.5%	2.5%	4.4%
D5 Reviewing fees and charges	0.7%	0.0%	1.2%	0.1%
T&C and changes to T&C (KP5, D4, D17)	**3.8%**	**0.3%**	**0.3%**	**2.0%**
Provision of customer owned banking service	**38.2%**	**35.5%**	**5.1%**	**5.1%**
Third party products (D13)	18.1%	10.5%	0.6%	1.1%
Statement of accounts (D16)	1.4%	1.4%	3.3%	2.8%
Direct debits arrangements (D20)	1.6%	1.1%	0.6%	0.4%
Chargebacks (D21)	16.5%	21.5%	0.0%	0.5%
Recurring payment arrangements (D21.3)	0.2%	0.4%	0.5%	0.2%
Closure of accounts (D22)	0.2%	0.5%	0.2%	0.1%
Account combination (D26.4)	0.1%	0.1%	0.0%	0.0%
Provision of credit	**1.7%**	**2.4%**	**3.1%**	**4.4%**
Credit assessment (KP4, D6, D7)	1.0%	1.6%	2.6%	3.4%
Financial difficulties (KP4, D24)	0.2%	0.4%	0.2%	0.5%
Joint debtors, accounts and subsidiary cards (D9, D10, D11)	0.1%	0.0%	0.0%	0.1%
Other provision of credit obligations (D8, D12, D26)	0.4%	0.4%	0.3%	0.4%
Other Code obligations (such as Training, Privacy, IDR)	**17.8%**	**19.1%**	**27.1%**	**34.0%**
Privacy and confidentiality (KP5, D23)	12.1%	13.1%	20.0%	29.8%
Advertising (KP3, D1)	0.8%	1.3%	2.0%	2.1%
Communication (D15, D18, D25)	2.3%	2.9%	4.2%	0.9%
Training (KP5, D14. E2)	0.4%	0.6%	0.5%	0.5%
Dispute Resolution (KP6, D27, D28, D28, D30)	1.6%	0.6%	0.5%	0.6%
Promotion of the Code (B, KP10, E1)	0.5%	0.6%	0.0%	0.1%

Non-compliance with the privacy obligations in Key Promise 5 and Section D23 of the Code has grown steadily over the past four years. It was the most significant area of specific non-compliance in 2015–16, accounting for about one-third (30%) of self-reported breaches. Eight Code Subscribers each reported in excess of ten breaches of privacy obligations. Three Code Subscribers accounted for one-third (33%) of all privacy breaches, with each advising of more than 20 breaches.

Privacy breaches commonly involved the inadvertent disclosure of personal information to third parties, with human and processing errors typically identified as the primary cause. Remediation actions included staff counselling and training in privacy obligations, review of manual processes and reinforcement of authorisation levels.

Two other main areas of non-compliance were Key Promise 5 ('delivery of high customer service and standards') and Key Promise 8 ('compliance with legal and industry obligations'), which respectively made up 20% and 16% of breaches in 2015–16. These areas also accounted for a substantial proportion of non-compliance in previous years. Other areas contributing more than 5% of total self-reported Code breaches in 2015–16 included 'disclosure of interest rates, fees and charges' (Key Promise 3, Section D3 and Section D5) and 'provision of general information' (Key Promise 3, Section D2 and Section D19), each of which accounted for 75 breaches.

For a full comparative analysis table of all self-reported Code breach data from 2012–13 to 2015–16, see Appendix B and Appendix F. For de-identified examples of Code breaches self-reported by Code Subscribers, including breach details and remedial actions, see Appendix C.

Culture and framework of positive breach reporting

24 Code Subscribers (33%) reported nil Code breaches in 2015–16. **Table 4** shows self-reported Code breach numbers by institution size in 2015-16.

Table 4: Number of self-reported Code breaches by size of Code Subscriber

	Size of institution (measured by $ assets)					
Number of self-reported Code breaches	**Small (under $200m)**	**Medium ($200m to $500m)**	**Large ($500m to $1b)**	**Largest (over $1b)**	**Total**	***Total 2014-15 for comparison[5]***
Nil	16	4	3	1	**24**	***31***
1 to 10	8	10	6	3	**27**	***33***
11 to 20	1	2	3	2	**8**	***5***
21 to 50	0	0	2	7	**9**	***9***
51 to 100	1	0	1	3	**5**	***2***
Over 100	0	0	0	0	**0**	***0***
Total	26	16	15	16	**73**	***80***

Positive Code breach reporting increases with the size of the institution. The majority of small institutions (62% or 16) reported nil Code breaches, while the majority of medium to largest institutions reported Code breaches. From the 16 largest institutions, one reported nil Code breaches in comparison to ten which reported in excess of 20 Code breaches.

[5] Number of self-reported Code breaches for periods 2012-13 and 2013-14, see Table 16, page 46

For comparison and benchmarking purposes, **Table 5** provides the self-reported Code breach averages for each institution size.

Table 5: Total and average of self-reported Code breaches by size of Code Subscriber

	Size of institution (measured by $ assets)					
	Small (under $200m)	Medium ($200m to $500m)	Large ($500m to $1b)	Largest (over $1b)	Total	*Total 2014-15 for comparison*[6]
Total number of self-reported Code breaches	102	49	211	456	**818**	***646***
Average per institution	3.9	3.1	14.1	28.5	**11.2**	***8.1***

Over time, the Committee will use the collected data on self-reported Code breaches as a baseline for assessing trends in the future. It will also be used to benchmark individual institutions' performance against institutions of similar size (for example in 2015-16 a small institution reported an average of three Code breaches and a largest institution reported an average of 28 Code breaches).

The Committee will continue to assist Code Subscribers with their compliance processes and encourage positive breach and complaints monitoring and reporting to ensure that it is an accurate reflection of their performance.

Self-reported significant Code breaches

Code Subscribers also report through the ACS on 'significant breaches'. A **significant breach** of Code obligations is determined by reference to a number of factors including:

- similar breaches of this nature that have occurred within the Code Subscriber's organisation
- the number of customers affected
- the adequacy of organisational arrangements to ensure compliance with the Code
- the extent of customer detriment
- remedial actions and costs incurred, and
- the time period over which the breach occurred.

The Committee has been collecting significant breach data from Code Subscribers through the ACS program since 2012–13. The nature and extent of the identified significant Code breaches is an important indicator of Code compliance as, by definition, these Code breaches have the most impact on customers. Often these Code breaches, together with remedial actions taken by Code Subscribers, are reported to the Australian Securities and Investments Commission (ASIC). The role of the Committee is not to duplicate this regulatory action but to assist Code Subscribers to meet relevant Code obligations.

Seven Code Subscribers reported a total of 11 significant Code breaches in 2015–16, compared to five significant Code breaches reported by five Code Subscribers in 2014–15. One significant Code breach was reported by a medium institution, with the remaining significant Code breaches reported by largest institutions.

[6] Total and average of self-reported Code breaches for periods 2012-13 and 2013-14, see Table 15, page 46

Table 6 provides an overview of the areas in which the significant Code breaches were recorded. Significant Code breaches in 2015–16 reflected the same key areas of concern as non-significant self-reported Code breaches, particularly in regard to privacy obligations.

Table 6: Self-reported significant Code breaches by section 2015–16

	2015-16
General commitments	**2**
Key commitments (KP8)	**2**
KP8 We will comply with our legal and industry obligations	
Disclosure	**1**
Interest rates, fees and charges	**1**
D3 Information on interest rates, fees and charges	
Other Code obligations (such as Training, Privacy, IDR)	**8**
Advertising	**2**
D1 Advertising	
Dispute Resolution	**1**
D28 Our complaints handling process	
Privacy and confidentiality	**5**
D23 Information privacy and security	
Grand Total	**11**

Appendix D contains information on these significant Code breaches, including the status of remedial actions.

Code Subscribers’ compliance initiatives

Individual Code Subscribers introduced several initiatives to improve Code monitoring programs and reporting processes in 2015–16.These have strengthened compliance risk assessment processes and further embedded compliance requirements within institutions and across the industry. Initiatives included:

- reviewing and improving breach and complaint registers
- increasing internal oversight and analysis of breach and complaint registers
- providing Code refresher training for staff regularly or as needed, as well as training in specific areas such as complaint and dispute handling
- making the Code and compliance information readily accessible to all staff
- monitoring and supervising staff to improve their compliance performance, and providing tools such as compliance checklists
- conducting spot checks, audits and other internal compliance testing, including ‘mystery shopping’ exercises
- further embedding Code compliance and reporting in company frameworks and cultures – for example by ensuring policies and procedures align with the Code
- conducting regular compliance reviews as well as reviews of performance against specific Code provisions such as responsible lending
- reviewing documents, product terms and conditions, and website information to ensure that the Code is complied with and referenced where appropriate, and
- monitoring Code and regulatory developments, advising staff and updating systems, processes and documents accordingly.

Internal dispute resolution

The 2015–16 ACS collated data about Code Subscribers' internal dispute resolution (IDR). The Committee used this information to assess Code Subscribers' compliance with the dispute resolution obligations set out in the Code, in particular:

- Key Promise 6 – 'We will deal fairly with any complaints'
- Section D27 – 'Prompt, fair resolution of complaints', and
- Section D28 – 'Our complaints handling processes'.

Complaint numbers

89% of Code Subscribers self-reported 14,100 complaints handled through their IDR process. This is a 16% decrease from the 16,709 complaints reported in 2014–15. External dispute resolution (EDR) data also shows a decrease in complaints.

In its role as an EDR provider, FOS reported that it accepted 191 disputes against 'credit unions' in 2015–16,[7] down 36% from the 297 disputes reported in its previous review. The Credit & Investments Ombudsman (CIO) does not use the category 'credit unions'. Its 2014-15 Annual Report on Operations reports that 99 (2%) complaints were received against authorised deposit-taking institutions which include banks, mutual banks, building societies and credit unions.[8]

Table 7 identifies the number of self-reported complaints by size of institution.

Table 7: Number of self-reported complaints by size of institution

	Size of institution (measured by $ assets)					
Number of self-reported complaints	**Small (under $200m)**	**Medium ($200m to $500m)**	**Large ($500m to $1b)**	**Largest (over $1b)**	**Total**	***Total 2014-15 for comparison[9]***
Nil	7	1	0	0	**8**	***10***
1 to 10	12	5	1	1	**19**	***18***
11 to 20	4	1	2	2	**9**	***8***
21 to 50	1	5	3	2	**11**	***17***
51 to 100	2	1	4	2	**9**	***6***
101 to 1,000	0	3	5	5	**13**	***18***
Over 1,000	0	0	0	4	**4**	***3***
Total	**26**	**16**	**15**	**16**	**73**	***80***

Only eight (11%) institutions did not self-report complaints. These were mainly small institutions. One-third of institutions, regardless of size, reported in excess of 50 complaints each. Of the 16 largest institutions, four reported more than 1,000 complaints.

For comparison and benchmarking purposes, **Table 8** provides the self-reported complaint average for institutions of different sizes. Overtime, the Committee will use this data to promote a culture and framework of positive complaints reporting.

---

[7] FOS Annual Review 2015–16, page 60.
[8] CIO Annual Report on Operations 2014-15, page 39 (at the time of this report, the CIO had not published its figures for 2015-16)
[9] Number of self-reported complaints for periods 2013-14 and 2012-13, see Table 18, page 47

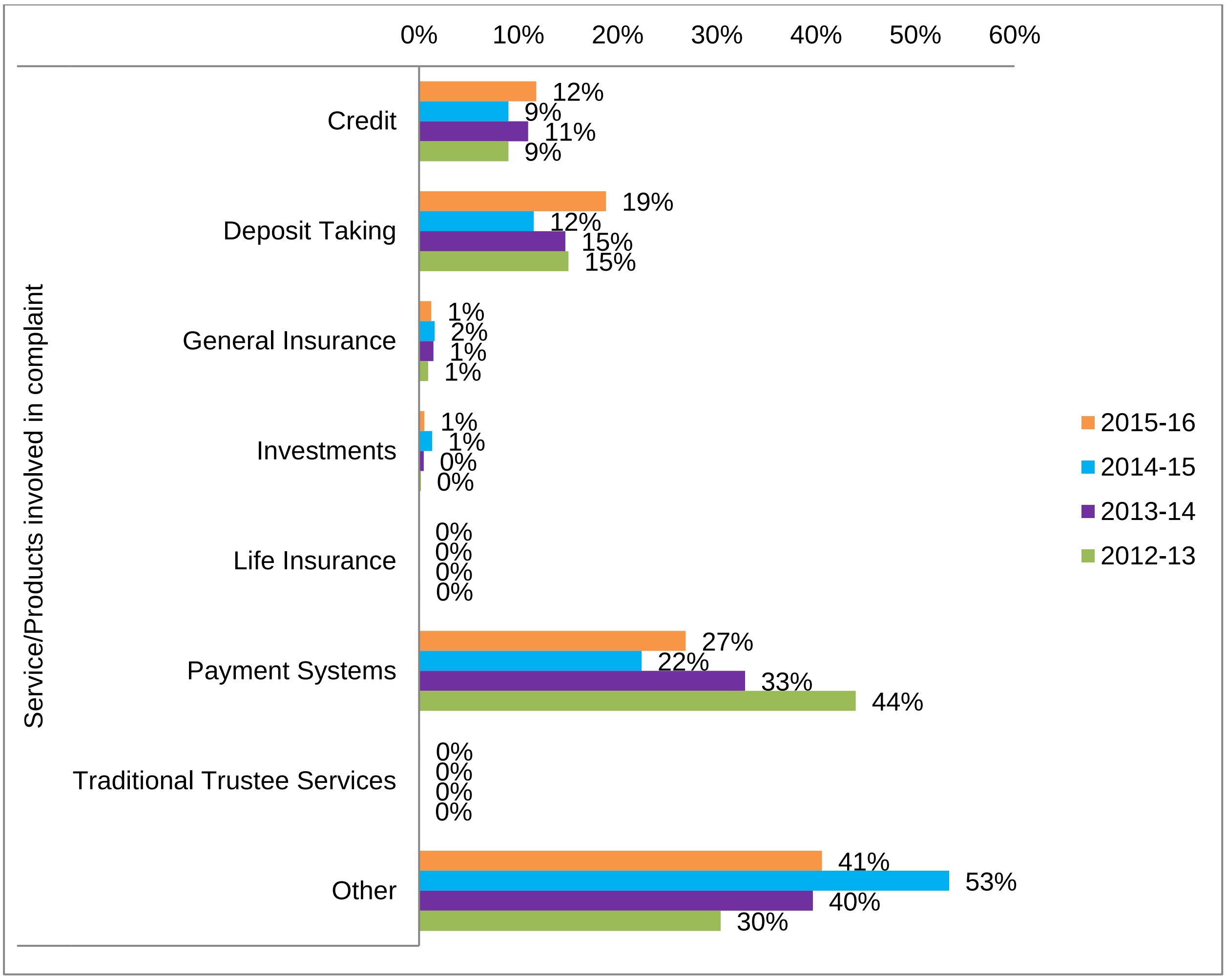
Institutions can draw comparisons with the average number of self-reported complaints by institutions of similar size (for example in 2015-16 a small institution reported an average of 13 complaints and a largest institution reported an average of 630 complaints). These figures are based on the self-reported breach data provided by the industry.

Table 8: Total and average of self-reported complaints by size of institution

	Size of institution (measured by $ assets)					
	Small (under $200m)	Medium ($200m to $500m)	Large ($500m to $1b)	Largest (over $1b)	Total	*Total 2014-15 for comparison*[10]
Total number of self-reported complaints	324	747	1,815	11,215	**14,100**	***16,709***
Average per institution	12.5	46.7	121	700.9	**193.2**	***208.9***

Complaint service/product areas

Chart 2: Percentage of complaints by service/product involved 2013–16[11]



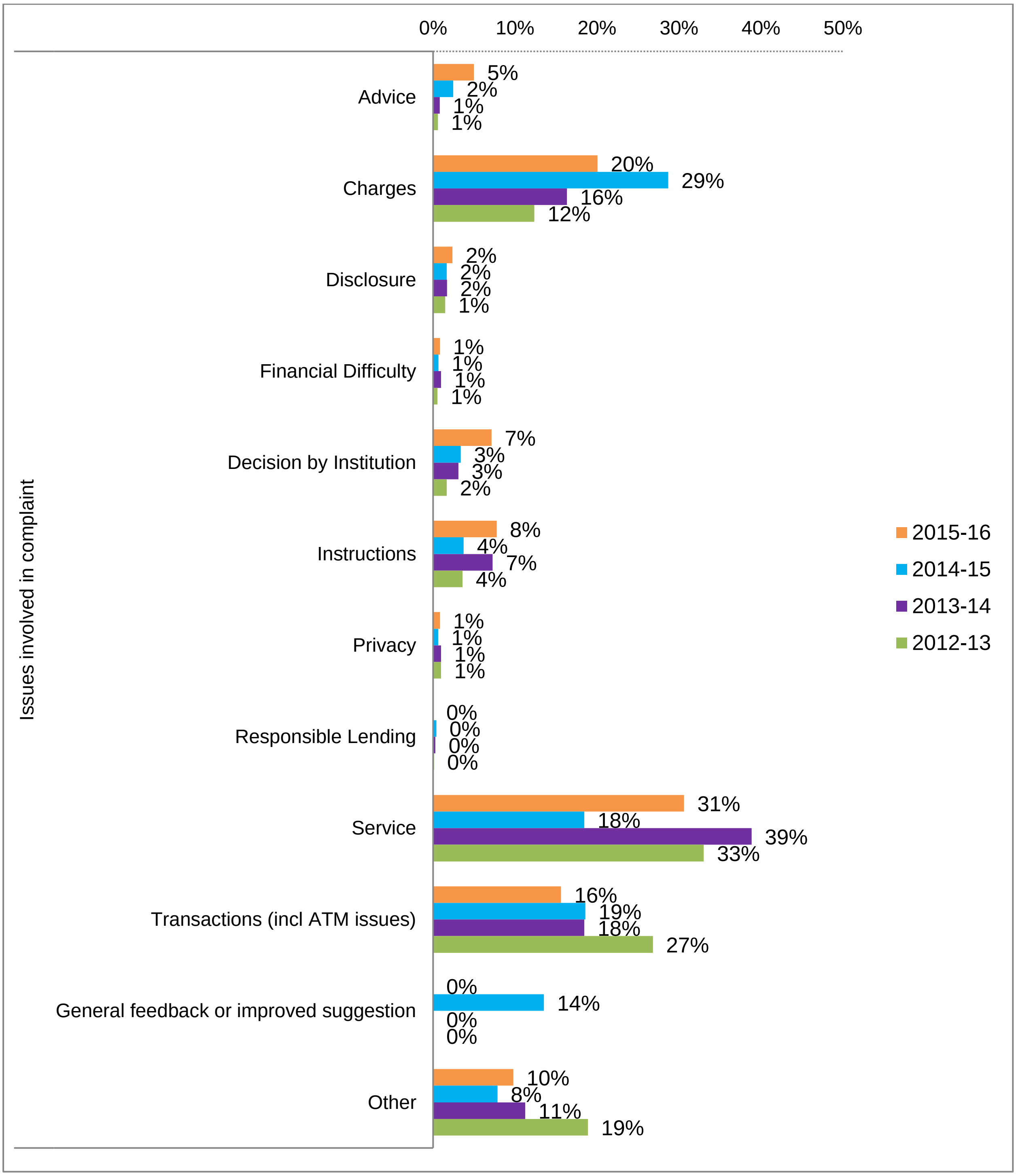
[10] Total and average of self-reported complaints by size of institution for 2013-14 and 2012-13, see Table 17, page 46

[11] 'Other' represents the number of complaints that were noted by the institution, but not further identified regarding the service/product involved.

The majority of complaints related to payment systems (27%), deposit taking (19%) and credit products (12%). Nevertheless, 41% of complaints were not categorised by product/service, a slight improvement compared to 53% uncategorised in 2015.

Complaint issues

Chart 3: Percentage of complaints by issues involved 2013–16[12]



[12] 'Other' represents the number of complaints that were noted by the institution, but not further identified regarding the issue involved.

Almost three in ten complaints (31%) related to service issues, mirroring the high number of Code breaches self-reported for Key Promise 5 (‘We will deliver high customer service and standards’). The other main complaint issues in 2015–16 were charges (20%) and transactions (including ATM issues) (16%). Interestingly, the high number of self-reported breaches of privacy obligations was not reflected in complaints, of which only 1% concerned privacy.

Overall, service complaints and technical issues continue to be the source of issues that are most reported by customers. Some key areas regarding the nature of complaints as reported by Code Subscribers included:

Loan products:

- Management of loans regarding loan applications.
- Level of service including processing and information provided relating to a customer being managed under a hardship arrangement.
- Default/perceived default listing with VEDA.
- Not complying with debt collection guidelines.

Credit card:

- Upgrade of credit card modules.
- Credit card being linked to incorrect savings account.

Deposit taking and payment systems:

- Deposit Taking and Payment Systems continue to be the source of most customer complaints.
- Combination of products and particular instructions that had not been followed correctly in relation to deposit taking, payment systems and investments.
- Term deposit early release term.
- Funds transferred to incorrect accounts or BSB.
- Unauthorised transaction due to internet related, ATM related, credit card related fraud or due to human error.
- ATM limit increase issue.
- Fraudulent cheque being credited to a customer’s account.

Fees and charges:

- Introduction of a new fee structure for transaction accounts.
- Amount and frequency with which certain fees were charged (such as coin handling, paper statement charges, overdrawn accounts, dishonoured Direct Debits).
- Withholding tax issue on deposit accounts.
- Customers wanted a better interest rate or were not happy with the exchange rate.
- Customer disputed that he did not receive information about a rate drop on one of his accounts.

IT issue:

- Issues with internet banking due to a change of the banking platform (such as interruption of services, preventing customer access).
- Implementation of a new digital internet banking solution caused dissatisfaction with the changes to functionality, particularly from the older demographic in the customer database.

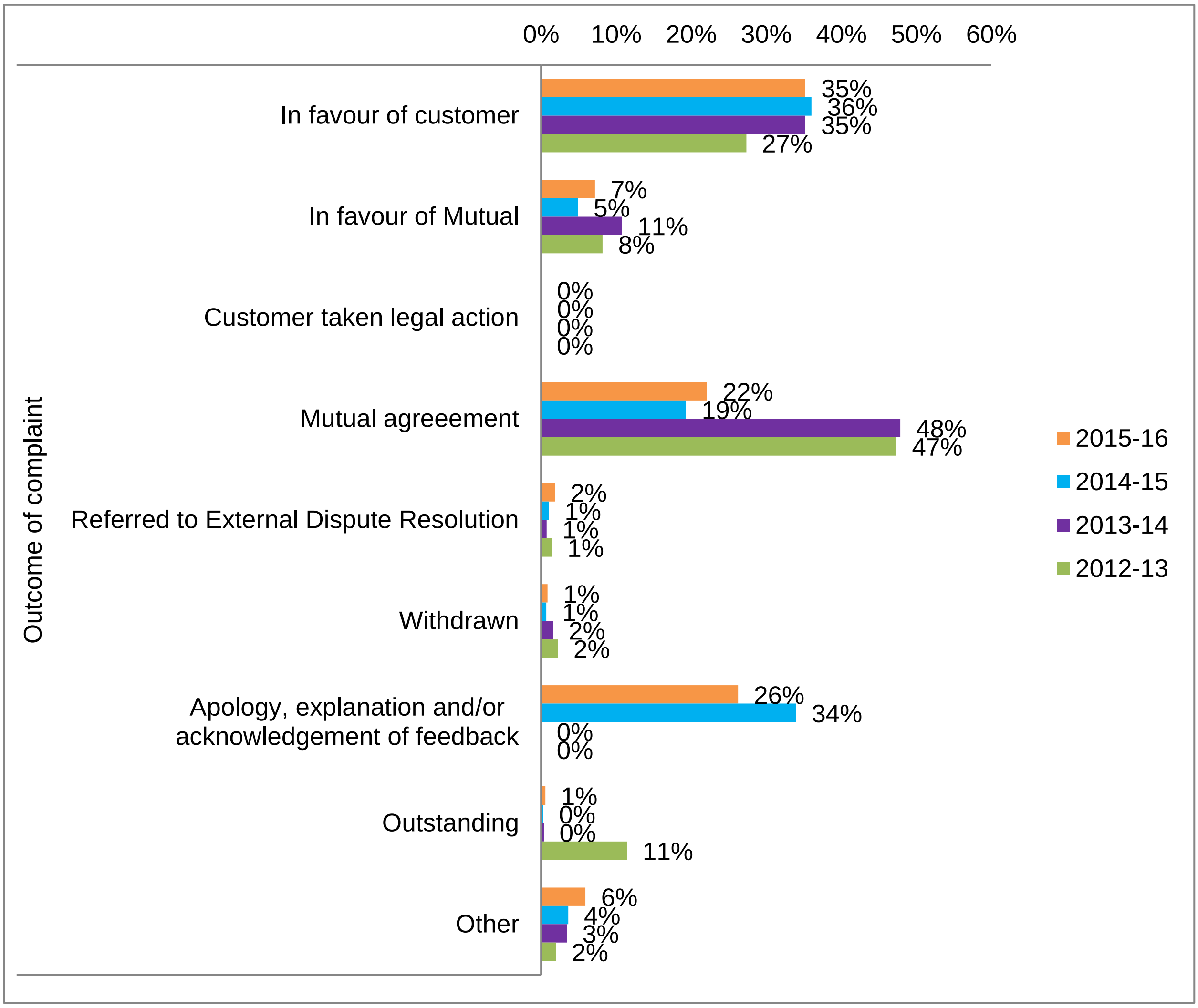
Service involved:

- Dissatisfaction with the phone interface (such as hold music).
- Branch closures.
- Complaints linked to changes in systems, products and processes following a merger.
- Customers expected a better level of service in some areas.
- Customer believed he was treated unreasonably based on the tone of communication received.
- Complaint about length of time to resolve a complaint.

Complaint outcomes

The ACS also collected information about how quickly and in what way institutions resolved complaints. **Chart 4** shows complaints by outcome for 2013 to 2016.

Chart 4: Percentage of complaints by outcome 2013–16[13]



[13] 'Other' represents the number of complaints that were noted by the institution, but not further identified regarding the outcome.

Around one in three complaints (35%) were resolved in favour of the customer in 2015–16, similar to the previous year. One-quarter of complaints (26%) were resolved as an apology, explanation and/or acknowledgement of feedback and one-quarter (22%) were resolved in mutual agreement.

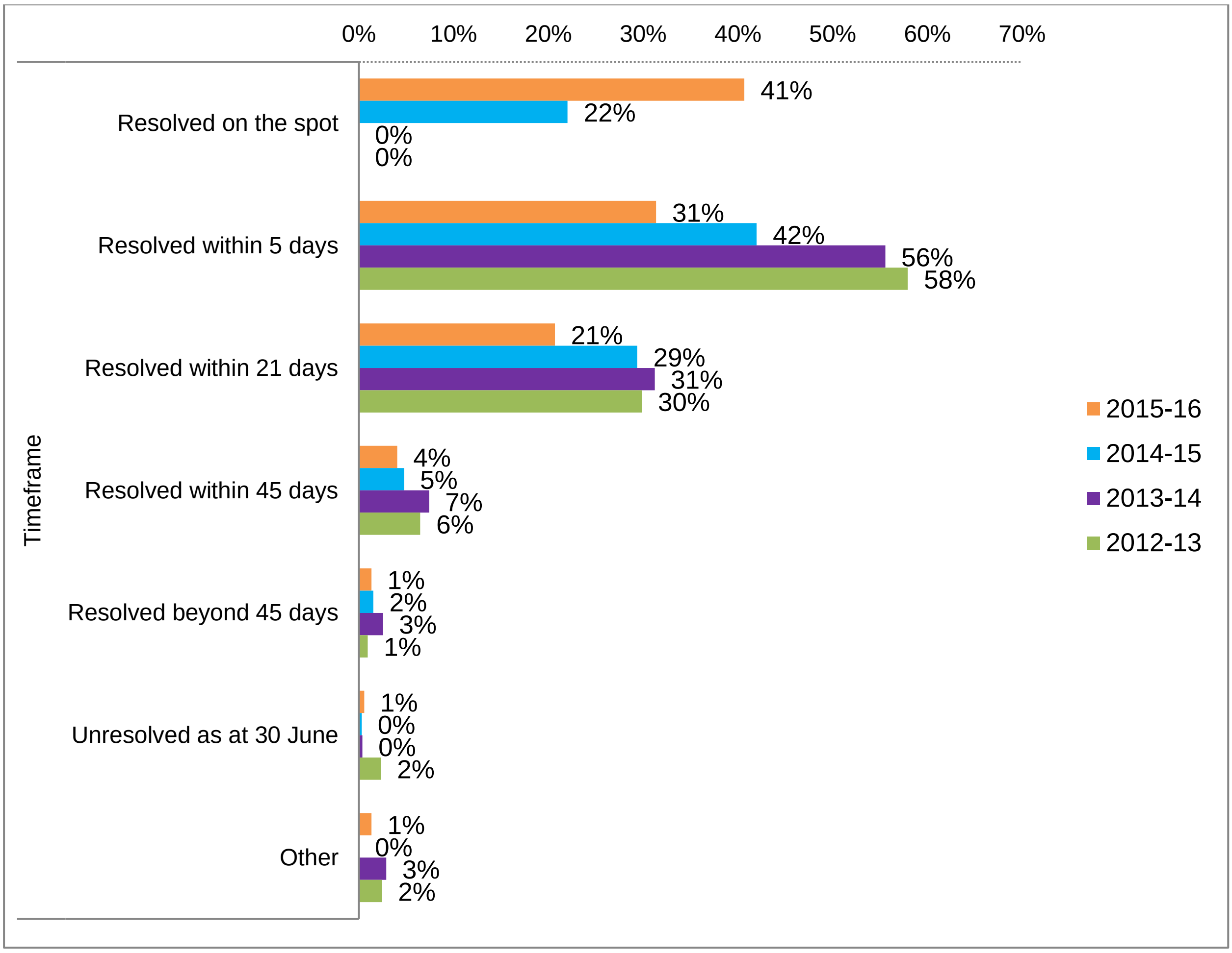
Examples provided by Code Subscribers for the different categories regarding ‘outcomes’ included:

- ‘In favour of customer’ included refunds of charges in good faith.
- ‘In favour of customer’ included generally refund of fees.
- ‘Mutual Agreement’ included change of account type and waiver of fees.
- ‘General Feedback’ included explanation of fees or account structure.
- ‘Other’ complaints largely related to Australian Taxation Law and ATO guidance notes.

Complaint resolution timeframes

Chart 5 breaks down complaints by time taken to resolve.

Chart 5: Percentage of complaints by resolution time 2013–16[14]



[14] ‘Other’ represents the number of complaints that were noted by the institution, but not further identified regarding the timeframe.

The large majority of complaints (93%) were resolved within 21 days, an improvement on 79% in 2015. Only 1% of customer complaints took longer than the required 45 days to resolve, in which case they were referred to the EDR provider.

In addition to data on complaints as defined in ASIC *Regulatory Guide 165.81* (RG 165.81)[15], the Committee also sought information from institutions regarding complaints resolved 'on the spot'. Commendably, 88% of institutions confirmed that they do record complaints that are resolved 'on the spot', exceeding the legislative requirement to record complaints that are not resolved within five business days.

Table 9 shows how many institutions of the same size record complaints resolved 'on the spot'. There appears to be no difference based on the size of the institution.

Table 9: Recording of complaints resolved 'on the spot' by size of institution

	Do you record complaints resolved 'on the spot'?	
Size of institution	***Yes***	***No***
Small (under $200m assets)	23	3
Medium ($200m to $500m assets)	15	1
Large ($500m to $1b assets)	13	2
Largest (over $1b assets)	13	3
Total	**64**	**9**

Culture and framework of positive complaints reporting

Effectively handling customers' complaints in a professional and timely manner – including analysing their root causes – is important to maintaining the traditional leadership role of the customer owned banking industry, which is known for putting the interests of their customers first.

In addition to quantitative data, most Code Subscribers provided valuable comments and information about complaints. However, the Committee is concerned about the high number of complaints reported without identification of the product/service (41%) or issue (10%) involved.

For a full comparative analysis table of all self-reported complaints data from 2013–14 to 2015–2016, see Appendix E and Appendix F.

[15] As per RG 165.81 a complaint is an expression of dissatisfaction regarding a customer owned banking service where a response is explicitly or implicitly expected and has not been resolved to the customer's satisfaction within five business days (except hardship cases, where all instances are to be included).

ANNUAL COMPLIANCE STATEMENTS VERIFICATION PROGRAM

In addition to the ACS program, the Committee conducts an ACS Verification Program. This is designed to validate Code Subscribers' compliance programs, investigating how effectively they identify, report and remedy breaches of the Code. Participating Code Subscribers receive specific feedback on possible areas for improvement.

Objectives and conduct

The objectives of the ACS Verification Program were to:

- discuss any specific non-compliance issues that were reported in the 2015 ACS for the previous period (1 July 2014 to 30 June 2015)
- assist the Committee to understand how institutions manage and monitor their compliance with the Code, and
- share examples of good industry practice.

As the data from the 2015 ACS was only received by October 2015, the program was conducted in February 2016. It was conducted via 15–30 minute teleconferences with each participating Code Subscriber and one face-to-face meeting. Four institutions had more than one representative present during the telephone conference and the face-to-face meeting was with two representatives of the institution. All Code Subscribers were cooperative and actively engaged in discussion.

Discussions with Code Subscribers during the program covered:

- complaint and breach systems
- complaints handling
- Code breach identification and reporting
- staff training, and
- promotion of the Code.

Participants

12 Code Subscribers participated in the Verification Program. Code Subscribers were chosen on the basis of their 2015 ACS responses, which either included a self-reported significant Code breach, showed signs of inconsistent or inaccurate complaints and breach data reporting, or indicated a risk of non-compliance.

Participating Code Subscribers were geographically spread and varied in size.

Table 10: Size and location of participating Code Subscribers

	NSW	Qld	SA	Vic	Total
Small institution (up to $200m assets)	2	-	-	-	**2**
Medium institution ($200m to $500m assets)	1	-	1	1	**3**
Large institution ($500m to $1b assets	-	-	-	-	**-**
Largest institution (over $1b assets)	-	4	1	2	**7**
Total	**3**	**4**	**2**	**3**	**12**

Findings

All selected institutions confirmed that they maintained a complaints register. The formats of these varied: complaints registers could be an Excel spreadsheet, a component of the core banking system or contained in a separate IT system for complaints recording.

The majority of institutions recorded ‘Charges’, ‘Service’ and 'Transaction’ as the three main categories of complaints. Institutions advised that complaints about ‘Charges’ often related to fees or charges that the institution was entitled to charge but that the customer was unhappy with. Complaints regarding ‘Service’ could include staff dealings with a customer, as well as other concerns such as the timeliness of service. Complaints regarding transactions included internet banking system failures, as well as fraudulent or mistaken transactions.

All institutions confirmed that frontline staff receive training regarding complaints handling and dispute resolution and nine institutions advised that this training must be undertaken annually. Eight institutions reported that they record complaints that are resolved at the initial point of contact but still expressed some doubts that staff were doing this in all instances.

Five institutions reported that compliance staff review all complaints to assess whether there has been a breach of the Code; five institutions reported that they have a dedicated complaints or customer relations manager who assesses all complaints; and two institutions reported that staff are required to make this assessment themselves when registering a complaint.

Good industry practice

Institutions expressed positivity about the usefulness of breach reporting and complaints data. They reported that awareness of the utility of complaints analysis was extending beyond compliance teams to other parts of the institution.

Two examples of good industry practice were identified through the ACS Verification Program. Firstly, the majority of institutions are requiring all staff to complete annual refresher training on their obligations regarding breach reporting and complaints handling; this helps to keep the training fresh and enables more breaches and complaints to be captured. In addition to refresher training, some institutions are incorporating breach and complaint training into other training modules (e.g. privacy training) and communicating regularly to staff, by email or through the intranet, reminding them of the requirements and benefits of recording breaches and complaints.

Secondly, the majority of institutions are also recording all complaints, including those resolved on the spot. Institutions have spoken about the value of complaints recording to assessing any emerging trends or risks and gauging how customers are feeling about the institution and its processes. Institutions gave examples of how feedback gained by assessing easily resolvable complaints has helped them improve their processes e.g. reviewing the institution’s structure of fees based on feedback/complaints about its existing structure.

Investigations

The Charter and the Code empowers the Committee to investigate allegations from any person that a customer owned banking institution has breached the Code. The Committee is able to investigate instances of alleged non-compliance, and to identify and monitor emerging industry issues.

While the Committee cannot consider claims for compensation and loss, it can initiate Code investigations without needing a complaint to act as a trigger. These investigations are mainly used to identify and assess:

- whether a breach has occurred and its extent
- the broader and potential impacts of a breach
- the effect of non-compliance on the customer owned banking institution and its customers
- the root cause of the breach and whether it may be systemic or significant, and
- any remedial action proposed or taken by the customer owned banking institution.

While every investigation is unique, each aims to achieve compliance outcomes that improve customer owned banking standards.

Table 11: For institutions – how to respond to a review of an alleged Code breach

Following a review of an alleged Code breach, the Committee expects institutions to:
☑ Positively engage with the Committee
☑ Thoroughly review the incident to assess if it constitutes a breach of the Code
☑ Report the breach in the breach register (if a breach of the Code has occurred)
☑ Report the breach to executive management
☑ Identify all customers potentially affected by the events
☑ Assess if the breach is systemic and/or significant
☑ Take remedial action to address the causes of non-compliance
☑ Review and enhance processes and procedures
☑ Train staff

CASEWORK

In 2015–16 the Committee received three new matters for investigation: two from FOS EDR and one directly from the customer. The subsequent investigations are summarised in **Table 12** according to the Code sections considered in each case.

Table 12: Investigations registered in 2015–16

KP5 – We will deliver high customer service and standards **E2 – Training our staff**	**Issue:** The customer had Home Cover Policy insurance which was administered by the institution as the agent of the insurer. The customer's vehicle was broken into in a carpark whilst she was at work. The customer wanted to know whether she could lodge a claim for the items stolen from her vehicle under her home insurance policy. According to the customer, the institution provided conflicting information about her level of cover and whether the stolen items would be covered if she lodged a claim. **Outcome:** The institution provided conflicting information about the customer's insurance cover. However: • the customer was provided with the correct information about her level of cover on two occasions prior to the error • the error was caused by a crash of the system of the third party insurer • the institution apologised and corrected its error within the next day • the customer had a conversation with the institution about upgrading her level of cover to cover such a loss but was not satisfied • the customer did not receive any written communication from the institution to confirm that she had a policy which would have covered such a loss. The institution confirmed that it will review its procedures and processes relating to providing advice for insurance cover and handling of insurance claims. **Status**: Closed – determined Code breach.
KP4 – We will be responsible lenders **D26 – Debt collection and legal action**	**Issue:** The customer had a secured car loan with the institution. The customer declared himself bankrupt and the customer's loan with the institution was listed in the bankruptcy. The institution took possession of the secured vehicle, which was unregistered and uninsured. The customer then lodged a dispute with FOS and alleged that the institution did not provide him with appropriate financial difficulty assistance and breached the ASIC and Australia Competition and Consumer Commission *Debt Collection Guideline*. **Outcome:** The customer did not provide a privacy authority. The Committee agreed to close the matter and undertake a separate unidentified Own Motion Inquiry with the institution in regards to financial difficulty and IDR procedures in general. The Committee was satisfied with the outcome of the Own Motion Inquiry and the information provided by the institution relating to their financial difficulty and IDR procedures. **Status:** Closed – outside jurisdiction (no privacy authority).
KP3 – We will give you clear information about our products and services **KP5 – We will deliver high customer service and standards** **KP6 – We will deal fairly with any complaints**	**Issue:** The customer held a Home and Contents policy which was administered by the institution as the agent of the insurer. The customer alleged that the institution caused confusion by sending renewal notices containing discrepancies regarding the actual insurance cover. The customer also alleged that the institution did not escalate her complaint when she requested this. **Outcome:** The Committee determined that the institution had breached Key Promises 3, 5 and 6 and that remedial action undertaken by the institution was sufficient to minimise the reoccurrence of a breach. **Status:** Closed – determined Code breach.

Own Motion Inquiries

Own Motion Inquiries (OMI) are an important part of the Committee's work. These inquiries take a targeted, in-depth look at a particular area of Code standards, examining instances of both non-compliance and good industry practice. Based on the findings, the Committee develops specific guidance for Code Subscribers in order to assist improvement in their service standards and compliance.

COMMUNITY ENGAGEMENT

During May and June 2016, the Committee conducted an OMI into Code Subscribers' compliance with their obligations under Part C, Key Promise 9 of the Code. Through Key Promise 9, customer owned banking institutions promise to recognise their impact on the wider community. This key promise reflects the customer owned banking sector's commitment to serving its communities.

> ***Key Promise 9 – We will recognise our impact on the wider community***
>
> *The customer owned banking sector has a strong community focus. We will take account of the impact of our operations on staff, the communities we serve and our customers. We will promote community engagement and will contribute to community activities and projects.*

The Mutuals Industry Review 2016 published by KPMG in November 2016 notes that 'As customer-centric and community-based organisations, the mutuals are more than a financial institution, with competitive products and great personal service. The mutuals also put their profits back into their customers through active contribution to the communities and causes that are important to them'.[16]

The inquiry gathered information about which communities are being served by the customer owned banking industry, the methods of engagement, the focus and impact of the community engagement and how institutions embed community engagement in their business culture and framework. The findings and recommendations contained in this report do not address specific areas of Code non-compliance, but examine how institutions ensure compliance.

Data collection comprised a 14-question online questionnaire completed by all 73 Code Subscribers. All institutions expressed positive views about the Own Motion Inquiry into community engagement and engaged different parts of the institution to respond to the survey.

The Committee will release a report detailing findings and the Committee's recommendations in January 2017.

[16] See, https://home.kpmg.com/content/dam/kpmg/au/pdf/2016/mutuals-industry-review-2016-report.pdf, page 10

Engaging with stakeholders

In 2015–16, the Committee continued to engage with stakeholders to influence positive changes in industry behaviour, share our experience of Code compliance and highlight areas of good industry practice.

STAKEHOLDER LIAISON

Throughout 2015-16, the Committee and the Code Team attended stakeholder liaison meetings with regulators, Code Subscribers, consumer and small business representatives, COBA and other customer owned banking cluster groups. Issues discussed included obligations under the Code, training and Code monitoring and compliance.

Industry

The Committee supported Code awareness by attending COBA's Conference in Darwin in September 2015 and COBA's stakeholder function in Sydney in October 2015. The Committee also had various meetings with COBA, its Chair and some industry cluster groups on development of an industry liaison group to share Committee updates and gather industry feedback. The Code Team also took part in COBA's Compliance Forums in Sydney, Brisbane, Adelaide and Melbourne in April and May 2016, presenting on Code issues and, in particular, highlighting the differences between Code compliance monitoring activities and FOS EDR investigation matters.

In October 2015, the Code Team also liaised with small business by presenting at the Small Business Development Conference in Melbourne and participating in a panel discussion at the Risk Culture and Regulation Conference in Sydney.

Consumer advocates

The Committee via its Code Team strengthened its relationship with consumer advocates by attending or presenting at the following events:

- Financial and Consumer Rights Council (FCRC) Conference in Torquay in September 2015
- Code Training day for financial counsellors in Melbourne in November 2015
- new premises launch for consumer community legal centres, the Consumer Action Law Centre, FCRC and Financial Counselling Australia (FCA) in Melbourne in December 2015
- Financial Counsellors' Association of Queensland Conference in Brisbane in March 2016
- financial legal rights centres meeting in Sydney in May 2016, and
- FCA Conference in Adelaide in May 2016.

Other

The Committee and Code Team kept up-to-date with regulatory matters by attending the ASIC Forum in Sydney in March 2016. The General Manager also attended the Governance Risk & Compliance Institute Conference in Melbourne in October 2015.

Meetings were facilitated for the four code committees (insurance brokers, general insurance, banking and customer owned banking) managed by the Compliance Manager. Following a meeting for all independent chairs in May 2015, separate meetings of consumer representatives and industry representatives were held in September and November 2015 respectively. These meetings were valuable to discuss, share and compare compliance monitoring issues among the various financial services industry sectors and to benefit from each other's experiences and ideas.

PUBLICATIONS

The Committee's website (www.cobccc.org.au), the Customer Owned Banking Association's website (www.customerownedbanking.asn.au/consumers/cobcop) and the FOS website (www.fos.org.au/about-us/codes-of-practice/) detail Code obligations and the Committee's role, functions and work program.

Early in 2016, the Committee reviewed and updated its website to include specific information for consumers and Code Subscribers. Consumer content includes information:

- about rights under the Code, including the rights of consumers in financial difficulty
- about how to report a concern, and
- for small business.

For Code Subscribers, the website now has specific guidance on Code compliance regarding financial difficulty obligations, advertising standards and direct debit arrangements. Fact sheets in the 'News and Publications' section provide training examples for staff.

During 2015–16, the Committee published:

- four editions of the *Accomplish* e-newsletter, keeping stakeholders up-to-date with activities and Code compliance news (editions 24–27)
- one news *Bulletin* (edition 56) announcing the appointment of the General Manager Code Compliance and Monitoring, Sally Davis
- an updated *Code Toolkit*, a handy pocket-sized reference guide for financial counsellors, and
- articles in *The Circular*, FOS's online magazine (editions 22–25).

2016–17: Future outlook

Throughout 2015–16 we considered how we can improve our communication with Code Subscribers, including raising awareness of the Code and sharing experiences of Code compliance. We were trying to actively seek feedback from the industry and work together to identify any areas for improvement.

In 2016–17, we will continue to improve Code monitoring. We will further refine the ACS process with the online portal and use the ACS Verification process to talk to and assist individual Code Subscribers. To guide good industry practice, we will continue to provide case studies as examples. We will also develop a benchmark document for the largest institutions in regards to their breach and complaints reporting in comparison to institutions of similar size and the industry in total.

In the investigations space, we will develop an Own Motion Inquiry in an area of emerging risk based on the 2016 ACS data and other relevant industry issues.

In the coming year we will maintain a focus on our communication and engagement strategy. We will continue to work closely with COBA and industry representatives from other customer owned banking industry discussion groups to obtain feedback and discuss how we can improve the impact of our monitoring and compliance work. We will also develop an online e-learning module on Code issues and, working with FOS EDR, contribute to any customer owned banking training activities.

Appendix A: Code Subscribers as at 30 June 2016

Australian Central Credit Union Ltd
    t/as People's Choice Credit Union
Bankstown City Credit Union Ltd
Big Sky Building Society Ltd
CAPE Credit Union Ltd
Central Murray Credit Union Ltd
Central West Credit Union Limited
Coastline Credit Union Ltd
Community Alliance Credit Union Limited
    t/as Catalyst Mutual
    t/as Illawara Credit Union
    t/as Western City Credit Union
Community CPS Australia Limited
    t/as Beyond Bank
Community First Credit Union Limited
Regional Australia Bank
    t/as Community Mutual Ltd
    t/as Hunter Mutual
    t/as New England Mutual
    t/as Orana Mutual
Credit Union Australia Ltd
    t/as CUA
Credit Union SA Limited
Dnister Ukrainian Credit Co-Operative Ltd
ECU Australia Ltd
EECU Limited
Family First Credit Union Limited
Fire Brigade Employees' Credit Union
Fire Service Credit Union Ltd
Firefighters & Affiliates Credit Co-operative Limited
    t/as Firefighters Credit Union
First Choice Credit Union Ltd
First Option Credit Union Limited
Ford Co-operative Credit Society Limited
Gateway Credit Union Ltd
Goulburn Murray Credit Union Co-Operative Ltd
Greater Bank
Heritage Bank Limited
Heritage Isle Credit Union Ltd
Holiday Coast Credit Union Ltd
Horizon Credit Union Ltd
Hume Bank Limited
Intech Credit Union Ltd
    t/as Intech Credit Union
    t/as Telstra Credit Union
Laboratories Credit Union Limited
Lysaght Credit Union Ltd
Macarthur Credit Union Ltd
    t/as The Mac
Macquarie Credit Union Ltd
Maitland Mutual Building Society Ltd
    t/as The Mutual
Maritime Mining & Power Credit Union Limited
    t/as Maritime Mining & Power Credit Union
    t/as Reliance Credit Union
    t/as Collie Miners Credit Union
MCU Limited
    t/as Maleny Credit Union
mecu Limited
    t/as Bank Australia
My Credit Union Limited
Northern Inland Credit Union Ltd
Nova Credit Union Limited
Orange Credit Union Limited
Police and Nurses Limited
    t/as P&N Bank
Police Bank Ltd
    t/as Police Bank
    t/as Customs Bank
Police Credit Union Limited
Police Financial Services Limited
    t/as BankVic

Pulse Credit Union Ltd
  t/as Pulse Credit Union
  t/as La Trobe University Credit Union
  t/as Melbourne University Credit Union
QPCU Limited
  t/as QBANK
QT Mutual Bank Limited
Quay Credit Union Ltd
Qudos Mutual Limited
  t/as Qudos Bank
Queensland Country Credit Union Limited
Queenslanders Credit Union Limited
Railways Credit Union Ltd
  t/as myMOVE
Select Encompass Credit Union Limited
SGE Mutual Limited
  t/as G&C Mutual Bank
South West Credit Union Co-operative Ltd
South West Slopes Credit Union Ltd
Southern Cross Credit Union Ltd
Summerland Credit Union Limited
Sydney Credit Union Ltd
Teachers Mutual Bank Limited
  t/as Teachers Mutual Bank
  t/as UniBank
The Broken Hill Community Credit Union Ltd
The Capricornian Ltd
Traditional Credit Union Ltd
Transport Mutual Credit Union Ltd
Victoria Teachers Limited
  t/as Victoria Teachers Mutual Bank
Warwick Credit Union Ltd
WAW Credit Union Co-operative Ltd
Woolworths Employees Credit Union Limited
Wyong Shire Credit Union Ltd

Table 13: Code Subscribers by State (head office) and size of institution[17]

	NSW	NT	QLD	SA	TAS	VIC	WA	Total	*Comparison to 2014-15[18]*
largest institution (over $1b assets)	7	0	4	1	0	3	1	**16**	*21*
large institution ($500m to $1b assets)	10	0	2	2	0	1	0	**15**	
medium institution ($200m to $500m assets)	10	0	4	0	0	2	0	**16**	*25*
small institution (up to $200m assets)	13	1	1	2	1	8	0	**26**	*34*
Total	**40**	**1**	**11**	**5**	**1**	**14**	**1**	**73**	*80*
Comparison to 2014-15	*44*	*1*	*12*	*5*	*1*	*16*	*1*	*80*	

[17] Institutions are counted by Australian Financial Service License.
[18] Following consultation with COBA and industry in 2015, we introduced new categories do define size of institutions based on assets (prior to that size of institutions were measured by number of staff):

Size of institution	prior 2016 measured by staff number	2016 Measured by $ assets
largest institution	n/a	over $1b assets
large institution	over 100 full time equivalent staff	$500m to $1b assets
medium institution	31-100 full time equivalent staff	$200m to $500m assets
small institution	up to 30 full time equivalent staff	up to $200m assets

Appendix B: Comparative table of self-reported Code breaches

	2012-13		2013-14		2014-15		2015-16	
	Total	Sig	Total	Sig	Total	Sig	Total	Sig
General	**297**	**4**	**277**	**2**	**359**	**2**	**392**	**2**
Key commitments	**287**	**3**	**256**	**2**	**318**	**1**	**338**	**2**
KP1 Be fair and ethical	0	0	2	0	26	0	3	0
KP2 Focus on our customers	41	0	21	0	20	0	27	0
KP5 Deliver high customer service	166	0	127	0	162	0	166	0
KP7 Recognise our customers' rights	0	0	0	0	0	0	3	0
KP8 Comply with legal & ind. obligations	79	3	89	2	110	1	130	2
KP9 Recognise impact on community	1	0	17	0	0	0	9	0
Provision of general information	**10**	**1**	**21**	**0**	**41**	**1**	**54**	**0**
Disclosure	**91**	**3**	**67**	**1**	**59**	**0**	**70**	**1**
Interest rates, fees and charges	**56**	**2**	**65**	**0**	**57**	**0**	**54**	**1**
KP3 Clear information	27	0	29	0	33	0	17	0
D3 Interest rates, fees and charges	23	2	36	0	16	0	36	1
D5 Reviewing fees and charges	6	0	0	0	8	0	1	0
T&C and changes to T&C	**35**	**1**	**2**	**1**	**2**	**0**	**16**	**0**
KP5 Deliver high customer service	0	0	0	0	0	0	7	0
D4 Fair terms and conditions	25	0	0	0	0	0	4	0
D17 Notifying changes to your account	10	1	2	1	2	0	5	0
Provision of customer owned banking service	**350**	**1**	**284**	**0**	**33**	**1**	**42**	**0**
D13 Third party products	166	0	84	0	4	0	9	0
D16 Statement of accounts	13	1	11	0	21	1	23	0
D20 Direct debit arrangements	15	0	9	0	4	0	3	0
D21 Chargebacks	151	0	172	0	0	0	4	0
D21.3 Recurring payment arrangements	2	0	3	0	3	0	2	0
D22 Closure of accounts	2	0	4	0	1	0	1	0
D26.4 Account combination	1	0	1	0	0	0	0	0
Provision of credit	**16**	**1**	**19**	**0**	**20**	**0**	**36**	**0**
Credit assessment	**9**	**1**	**13**	**0**	**17**	**0**	**28**	**0**
KP4 We will be responsible lenders	3	1	4	0	2	0	7	0
D6 Responsible lending practices	6	0	9	0	15	0	20	0
D7 Credit limit increase offers	0	0	0	0	0	0	1	0
Financial difficulties	**2**	**0**	**3**	**0**	**1**	**0**	**4**	**0**
KP4 We will be responsible lenders	0	0	0	0	0	0	1	0
D24 If you are in financial difficulties	2	0	3	0	1	0	3	0

Joint debtors, accounts & sub. cards	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**
D9 Joint accounts	1	0	0	0	0	0	0	0
D10 Subsidiary cards	0	0	0	0	0	0	0	0
D11 Safeguards for co-borrowers	0	0	0	0	0	0	1	0
Other provision of credit obligations	**4**	**0**	**3**	**0**	**2**	**0**	**3**	**0**
D8 Reverse mortgage loans	0	0	0	0	0	0	0	0
D12 Safeguard for loan guarantors	2	0	0	0	1	0	2	0
D26 Debt collection and legal action	2	0	3	0	1	0	1	0
Other Code obligations (such as Training, Privacy, IDR)	**163**	**7**	**153**	**3**	**175**	**2**	**278**	**8**
Privacy and confidentiality	**111**	**1**	**105**	**1**	**129**	**2**	**244**	**5**
KP5 Deliver high customer service	0	0	0	0	0	0	46	0
D23 Information privacy and security	111	1	105	1	129	2	198	5
Advertising	**7**	**1**	**10**	**1**	**13**	**0**	**17**	**2**
KP3 Clear information	0	0	0	0	0	0	4	0
D1 Advertising	7	1	10	1	13	0	13	2
Communication	**21**	**0**	**23**	**1**	**27**	**0**	**7**	**0**
D15 Timely, clear and effective	12	0	20	0	21	0	4	0
D18 Electronically	9	0	2	1	6	0	3	0
D25 Working with your representative	0	0	1	0	0	0	0	0
Training	**4**	**0**	**5**	**0**	**3**	**0**	**4**	**0**
KP5 Deliver high customer service	0	0	0	0	0	0	1	0
D14 Use of finance brokers	0	0	0	0	0	0	0	0
E2 Training our staff	4	0	5	0	3	0	3	0
Dispute Resolution	**15**	**0**	**5**	**0**	**3**	**0**	**5**	**1**
KP6 Deal fairly with any complaints	6	0	0	0	0	0	0	0
D27 Prompt, fair resolution of complaints	4	0	3	0	0	0	5	0
D28 Our complaints handling process	5	0	1	0	2	0	0	1
D29 External Dispute Resolution (EDR)	0	0	1	0	1	0	0	0
D30 Complaints about Code breaches	0	0	0	0	0	0	0	0
Promotion of the Code	**5**	**5**	**5**	**0**	**0**	**0**	**1**	**0**
B Commitment to comply with Code	3	1	0	0	0	0	0	0
KP10 Support and promote Code	1	0	0	0	0	0	1	0
E1 Publicising the Code	1	4	5	0	0	0	0	0
Grand Total	**917**	**16**	**800**	**6**	**646**	**5**	**818**	**11**

Appendix C: Examples of self-reported Code breaches in 2015-16

Breach details	***Remedial actions***
C1 We will be fair and ethical in our dealings with you	
Charge of incorrect customer fees.	Customer fees reversed and review of all business accounts to ensure no other customer was affected.
C3 We will give you clear information about our products and services	
It was identified that the minimum repayment warning disclosure contained in the customer's statements was incorrect.	As per legal advice the matter was recorded as a breach and procedures updated to ensure adequate controls in place so as to not have this issue reoccur.
ABN did not appear on all relevant documents.	Improved document proofing procedures implemented to ensure required details such as ABN appear on relevant documents.
C5 We will deliver high customer service and standards	
Most breaches of the Code occurred through complaints from customers in relation to the processes of the credit union, staff not knowing the products, or poor service.	Training and counselling provided on breaches at an individual and organisational level, where appropriate depending on the type of breach. Procedures, processes and checklists revised or amended to ensure similar breaches are not encountered in the future.
C8 We will comply with our legal and industry obligations	
Separate instances of unauthorised access by staff and Payment Card Industry Data Security Standard (PCIDSS) non-compliance.	Staff have been counselled and a warning letter issued. Training modules for all staff have been updated to address the scenarios involved. In regards to PCIDSS non-compliance, the credit union is engaging with an external party to progress the outstanding issues of non-compliance.
The breaches reported are unrelated events and involve non-compliance with various legislative requirements.	Each breach was investigated at the time of notification, and actions put in place to remedy the breach and prevent further occurrences.
Multiple breaches of legislative and industry requirements.	Various preventative controls have been put in place depending upon the nature of non-compliance with legislative and industry obligations. For example: updating and clarifying procedures, staff training (including performance

Breach details	Remedial actions
	improvement plans) and amending of compliance checklists.
Breach was in relation to Australian Prudential Regulation Authority (APRA) APS 910. This Prudential Standard sets out the minimum requirements that a locally incorporated authorised deposit-taking institution (ADI) must meet to ensure that it is adequately prepared should it become a declared ADI for Financial Claims Scheme (FCS) purposes. In this instance a plan regarding how customer information would be captured in the event of a FCS declaration had not been sufficiently documented.	This has now been documented and will be considered annually as part of the credit union's reviews.
A breach concerned a late lodgement to APRA of a quarterly Housing Loan Return due to human error.	This has now been rectified.
A breach was a late lodgement to ASIC of a report on mistaken internet payments and unauthorised transactions as required under clause 44.1 of the *ePayments Code*.	This has now been rectified.
The breach related to the new *Anti-Money Laundering and Counter-Terrorism Financing Act* (AML/CTF) requirements of identifying and collecting information with respect to politically exposed persons and beneficial owners of entities.	The institution is in the process of redesigning its application forms to better cater for this requirement.
The multiple breaches related primarily to breach of legal and industry obligations (C8) and specifically around AML, privacy and disclosure obligations.	Generally, the preventative measures involved rectification, reminders of obligations, and where required, updating or creating new procedures and training.
D1 Advertising	
One breach was identified relating to an error in disclosure regarding notice periods for early redemptions from a Term Deposit. The institution's practice has been and remains to permit all Term Deposits to be immediately breakable however disclosure documents and the website contained references to notice periods for breaking Term Deposits over two years.	Disclosures have been amended to reflect the practices adopted by the institution. No customers were impacted, as no notice periods were imposed on any customer wishing to break a Term Deposit. The circumstances surrounding each breach were unique and not related. Controls have been introduced to prevent re-occurrence, including review of relevant processes and systems and update of procedure documentation, and counselling of staff.
D3 Information on interest rates, fees and charges	
Several instances where customers were complaining about transaction fees being charged.	Although staff were advising new customers of loyalty program fee structure and correct disclosure was being made it was recognised that more effort was required to ensure when opening accounts customers were made aware

Breach details	Remedial actions
	and confirmed their understanding of the fee structure and how to avoid being charged.
Multiple breaches were around staff ensuring that they take care when taking instruction from customers.	This area is being addressed through staff performance reviews etc.
D6 Responsible lending practices	
Breach in responsible lending practices.	This breach has resulted in a review and upgrade of the Lending Assessment process.
Senior manager attempted to approve a credit application in the absence of supporting financial documentation from applicant (against policy), where senior manager had no delegated authority to approve any applications.	Reported and escalated by loans manager, through reporting line to CEO. Following investigation, finalised with resignation of senior manager. Legal advice sought: issue was significant to us but not reportable to regulators. Evidence supporting credit application subsequently obtained and assessed and approved. This breach was self-detected.
D12 Safeguards for loan guarantors	
Issues with safeguards for loan guarantors.	Institution is currently in the process of amending its guarantor document pack to improve safeguards for loan guarantors.
D23 Information privacy and security	
Minor breach of privacy where a small amount of customers' *eStatements* were able to be seen by another small amount of customers.	Upon detection the error was quickly rectified with minimal impact. All affected customers were contacted and none of them wanted to make a formal complaint. The institution and its supplier have strengthened the controls.
Breaches were to do with mail house problems.	Mail house has introduced procedures to ensure breaches do not happen again. Staff training breach has been rectified.
Privacy breaches identified related to individual customers personal information being inadvertently disclosed to a third party (other customers). The primary cause of the breaches related to human processing errors.	Remedial actions have been taken to address the errors which include refresher training for impacted staff, apologies issued to impacted customers and instructions to incorrect recipients to discard/destroy the information received incorrectly.
Privacy breaches by service provider.	Preventative controls implemented included undertakings and obtaining independent audits of service provider procedures which led to a privacy breach.
Multiple breaches refer to breaches of employee privacy (payroll information and staff account visibility to non-authorised staff) and breaches of customer privacy by the accidental disclosure of another customer's statement to a customer.	The employee privacy breaches are being remediated at present by reinforcing authorisation levels in IT security systems. Breach of customer privacy was resolved through staff counselling and reviewing the manually produced statement process. Refresher privacy training to be conducted.
Statement sent to incorrect customer.	Statement re-sent to correct customer. Staff training completed to remind staff of internal procedures.

Breach details	***Remedial actions***
Privacy breaches.	On privacy breaches we have redeveloped our compliance induction which has a greater emphasis on privacy. In addition, we are currently developing privacy training which identifies the types of breaches occurring and what staff should do to minimise the risk of these breaches occurring.
The breaches reported were driven by human error and due to process.	In all instances of human error, parties have been individually addressed and where necessary, additional training provided. Where the matters related to process, the processes have been reviewed, amended where applicable and staff re-trained to mitigate re-occurrence of such breaches in future.
One customer received the statements of two other customers with her own statement.	Reported to mailing house and mailing house investigated. Occurred due to equipment control failure. No further incidents detected and not deemed systemic nor significant for regulator reporting. Customer did not wish to report issue as a complaint, merely alert us to the issue.
D26 Debt collection and legal action	
This breach was identified by a FOS Own Motion Review of credit listings which resulted from two FOS complaints in this regard.	As a result, a full independent review of five years of default listings was undertaken with corrections to listings completed by 30th June. Additionally, procedures were reviewed and altered and relevant staff have been retrained in the new procedures. A hindsight review program will be implemented going forward to ensure the new processes are being managed appropriately.

Appendix D: Significant self-reported Code breaches in 2015–16

KP8 'comply with legal and industry obligations'	
Issue	Failure to advise ASIC of changes to Responsible Managers. The cause of this involved a lack of documented policy and procedures regarding compliance with Financial Services Regulation (FSR) obligations around Responsible Managers.
Exposure	Significant Incident.
Outcome	The institution confirmed that this has now been addressed with implementation of policy and procedures to ensure awareness and compliance with FSR obligations regarding Responsible Managers.
KP8 'comply with legal and industry obligations'	
Issue	A group of loans (approximately 100 loans worth $26M) has been reported to APRA as Housing (predominantly Investor) instead of Commercial. The underlying cause was that the change control protocol was not followed, particularly checking with all affected stakeholders before implementing a change to business processes. Communication breakdown causing the decision made at Executive/relevant Committee not able to be considered by the Executive/relevant Committee preparing APRA reporting for business impact before it was implemented.
Exposure	Reportable Incident.
Outcome	Lending and Finance to be made more aware of outcomes of the relevant Committee decisions that are ratified by the Executive and due consideration given to impacts on business processes. Finance has implemented additional controls to ensure future reoccurrences are avoided.
D1 'Advertising'	
Issue	In relation to the institution's bonus saver account, misleading information was inadvertently provided to customers as the system parameters in relation to the bonus interest component of the product did not align with the Terms and Conditions in circumstances where the end of a calendar month fell on a weekend and not a working day. This was because the institution does not process on weekends. This resulted in some bonus saver account holders not receiving bonus interest when entitled to it (noting the reverse also applied and some holders did receive it when they should not have). The breach was caused due to insufficient testing of the product features against system parameters when the product was established.
Exposure	The breach was rated significant and reported to ASIC. It financially impacted numerous customers.
Outcome	All impacted customers were advised of the breach; advertising and Terms and Conditions were updated as appropriate; and all negatively impacted customers were placed back into the position they would have been in had the breach not occurred i.e. reimbursements were made. Even though numerous customers were financially impacted, the actual dollar value of reimbursement for each account holder was negligible to minor.

D1 'Advertising'	
Issue	In relation to a lending package, the institution advertised an insurance discount. The discount did not specify how long this was applied for and the institution believed this to be for as long as the customer held the package with the institution. This was the fair assumption to be made by customers based upon the content of the advertising; however, the institution's insurer only applied the discount to year one and not subsequent years. Therefore customers in this package may have been misled in terms of how long the discount was applicable for. The assumption being made as to how the discount worked without having this documented in the agreement with the insurer.
Exposure	The breach was rated significant and reported to ASIC. It financially impacted numerous customers.
Outcome	All impacted customers were advised of the breach; advertising and Terms and Conditions were updated as appropriate; and all negatively impacted customers were placed back into the position they would have been in had the breach not occurred i.e. reimbursements were made. Even though numerous customers were financially impacted, the actual dollar value of reimbursement for each account holder was negligible to minor.
D3 'Information on interest rates, fees and charges'	
Issue	The fees and charges schedule provided to customers of the institution contained two fees charged by the institution's transaction and clearing house service provider. The schedule explained the circumstances under which the fee would be charged and the institution described these as third party fees and that this is the cost charged to the institution. The fees included a customer Cheque Dishonour Fee and a Direct Debit Dishonour Fee. This description was correct at the time of publication. Subsequently, the service provider revised their fees and reduced them. However, the institution continued to charge the old fees and still described these as third party fees and the cost charged to the institution. As a result the fees and charges schedule was incorrect and possibly contained misleading or deceptive representations. The breach occurred due to oversight in the coordination of finance, operational and compliance functions when reviewing fees and documentation at least annually. None of the institution's own transactional fees were varied in the time period.
Exposure	The breach was reported to ASIC who subsequently advised that they were not going to investigate further at this stage. The breach report indicated possible breaches of the *ASIC Act* (Division 2 Part 2 s12DA - misleading and deceptive conduct, s12DB false and misleading representations) and COBCoP 3.1. The incorrect fees schedule was published on the institution's website and printed incorrectly for over two years. The institution determined that 631 customers were affected (such as charged these fees) in that period.
Outcome	All 631 customers were written to and reimbursed fees charged in full and interest (whether credit or debit interest) for the period in question. A comprehensive review of all fees (regardless of own, third party, lending or transactional) was completed. This was in turn reviewed by external auditors. Both fees have since been reduced and are no longer described as third party fees.
D23 'Information privacy and security'	
Issue	An existing staff member downloaded a number of sensitive documents via remote laptop access. The mobile device was not removed after it was known the employee would be leaving.
Exposure	Investigation determined that sensitive information had the potential to be sent to parties not connected to the institution including the media or customers.
Outcome	Employee was asked to return the information. A formal letter was sent detailing the institution's intention to pursue legal action if the employee would not comply. Current employees in sensitive roles are monitored electronically during their exit period.

D23 'Information privacy and security'	
Issue	Staff was sharing passwords. There was confusion regarding security obligations.
Exposure	Minor – there was little chance for financial/reputational loss, owing to the fast remedy applied. No impact on customers.
Outcome	Staff training and updates to inductions.
D23 'Information privacy and security'	
Issue	Credit card details emailed to wrong customer due to error in email recipient.
Exposure	Significant – potentially high amounts of financial/reputational loss. There was no financial loss and only affected one customer.
Outcome	Procedure updated to complete checking before credit card contracts are sent.
D23 'Information privacy and security'	
Issue	Breach of customer privacy due to data entry errors where staff have been incorrectly making changes to an unrelated customer's account and incorrectly released customer information to another customer as a result of not following procedures. Breach was caused by inadequate system controls which would force staff to check or confirm they have keyed in the correct customer's details before transacting on their account.
Exposure	Over the past 18 months 17 incidents of this nature have been identified. Each incident was small in itself as only one customer was impacted, though taken collectively the incidents pointed to a systemic issue.
Outcome	Required staff to search customer's account by name instead of account number until core banking system change is developed which would force staff to use this approach. Once completed it would remove the risk of keying in the wrong customer. Incident also reported to ASIC.
D23 'Information privacy and security'	
Issue	Breach of customer privacy due to the incorrect reporting of customer's overdraft application as a credit card application to a credit bureau. The error may have up to a 10 point impact to a customer's credit score when applying for further credit. Breach caused by incorrect system coding which resulted in the use of the wrong code when reporting credit applications to a credit bureau.
Exposure	The issue appeared to have been occurring for the past five years and has impacted around 3,000 customers.
Outcome	Completed system changes to correct records of customer overdraft applications. Arranged with the credit bureau to correct all records. Written to all impacted customers explaining the error. Institution also voluntarily reported the matter to the Privacy Commissioner.
D28 'Our complaints handling process'	
Issue	An independent Risk and Compliance review identified that the institution is unable to evidence its compliance with obligations RG165.90, RG165.91 and RG165.108. The review has determined a failure to retain key customer correspondence, including complaint resolution letters (for complaints exceeding 5 days in age) and final response letters, issued at either or both 21 and 45 days. The cause of the issue relates to inadequate control and monitoring arrangements supporting the process.
Exposure	Whilst the number of breaches in the institution's view, represent only a small number of customers (44 instances impacting 38 customers), the defects per opportunity indicate that the current compliance arrangements to ensure compliance with these requirements is inadequate.
Outcome	The institution has undertaken actions to improve its internal procedures, training of staff, increased monitoring of complaint inventory and implementation of Line 1 and Line 2 controls.

Appendix E: Comparative table of self-reported complaints

	Category	2012-13		2013-14		2014-15		2015-16	
Service/Products involved in complaints	Credit	1,345	*9%*	1,325	*11%*	1,608	*9%*	1,665	*12%*
	Deposit Taking	2,166	*15%*	1,829	*15%*	1,930	*12%*	2,655	*19%*
	General Insurance	132	*1%*	180	*1%*	263	*2%*	175	*1%*
	Investments	29	*<1%*	68	*<1%*	230	*1%*	76	*1%*
	Life Insurance	13	*<1%*	5	*<1%*	0	*0%*	3	*<1%*
	Payment Systems	6,334	*44%*	4,075	*33%*	3,746	*22%*	3,789	*27%*
	Traditional Trustee Services	0	*0%*	4	*<1%*	6	*<1%*	11	*<1%*
	Other[19]	4,374	*30%*	4,923	*40%*	8,926	*53%*	5,726	*41%*
Issues involved in customer complaint	Advice	84	*1%*	100	*1%*	413	*2%*	705	*5%*
	Charges	1779	*12%*	2,026	*16%*	4,792	*29%*	2,829	*20%*
	Disclosure	211	*1%*	211	*2%*	279	*2%*	334	*2%*
	Financial Difficulty	78	*1%*	122	*1%*	109	*1%*	117	*1%*
	Decision by institution	239	*2%*	383	*3%*	565	*3%*	1,005	*7%*
	Instructions	517	*4%*	903	*7%*	624	*4%*	1,093	*8%*
	Privacy	140	*1%*	121	*1%*	103	*1%*	118	*1%*
	Responsible Lending	15	*<1%*	35	*<1%*	65	*<1%*	0	*0%*
	Service	4,752	*33%*	4,822	*39%*	3,083	*18%*	4,318	*31%*
	Transactions (incl. ATM issues)	3,859	*27%*	2,291	*18%*	3,104	*19%*	2,201	*16%*
	General feedback or improvement suggestion	n/a	n/a	n/a	n/a	2,259	*14%*	0	*0%*
	Other	2,719	*19%*	1,395	*11%*	1,313	*8%*	1,380	*10%*
Outcome of customer complaint	In favour of customer	3,935	*27%*	4,371	*35%*	6,022	*36%*	4,968	*35%*
	In favour of institution	1,181	*8%*	1,335	*11%*	822	*5%*	1,013	*7%*
	Customer taken legal action	1	*<1%*	1	*<1%*	8	*<1%*	3	*<1%*
	Mutual agreement	6,812	*47%*	5,941	*48%*	3,228	*19%*	3,117	*22%*
	Referred to External Dispute Resolution	206	*1%*	92	*1%*	177	*1%*	258	*2%*
	Withdrawn	322	*2%*	199	*2%*	119	*1%*	123	*1%*
	Apology, explanation and/or acknowledgement of feedback	n/a	*n/a*	n/a	*n/a*	5,675	*34%*	3,704	*26%*
	Other	289	*2%*	425	*3%*	608	*4%*	834	*6%*
	Outstanding	1,647	*11%*	45	*<1%*	50	*<1%*	80	*1%*

[19] 'Other' represents the number of complaints that were not further specified by institutions.

	Category	2012-13		2013-14		2014-15		2015-16	
Timeframe	Resolved on the spot	8,338	*58%*	6,894	*56%*	3,681	*22%*	5,738	*41%*
	Resolved within 5 days	8,338	*58%*	6,894	*56%*	7,016	*42%*	4,423	*31%*
	Resolved within 21 days	4,299	*30%*	3,834	*31%*	4,909	*29%*	2,917	*21%*
	Resolved within 45 days	932	*6%*	920	*7%*	797	*5%*	571	*4%*
	Resolved beyond 45 days	135	*1%*	317	*3%*	256	*2%*	185	*1%*
	Unresolved as at 30th June	337	*2%*	45	*<1%*	50	*<1%*	80	*1%*
	Other	352	*2%*	359	*3%*	0	*0%*	186	*1%*
Number of complaints which include Code breaches		309	*2%*	370	*3%*	233	*1%*	256	*2%*
Total number of complaints		14,393		12,409		16,709		14,100	
Number of institutions that reported complaints		82	*90%*	79	*89%*	70	*88%*	65	*89%*

Appendix F: Additional tables – breach & complaints data

Table 14: Total number of Code Subscribers by size of institution

<table>
<tr><th></th><th>2012–13</th><th>2013–14</th><th>2014–15</th><th>2015–16[20]</th></tr>
<tr><th></th><th>Total</th><th>Total</th><th>Total</th><th>Total</th></tr>
<tr><td>Total number of institutions</td><td>91</td><td>89</td><td>80</td><td>73</td></tr>
<tr><td>- largest institutions</td><td rowspan="2">22</td><td rowspan="2">22</td><td rowspan="2">21</td><td>16</td></tr>
<tr><td>- large institutions</td><td>15</td></tr>
<tr><td>- medium institutions</td><td>28</td><td>28</td><td>25</td><td>16</td></tr>
<tr><td>- small institutions</td><td>41</td><td>39</td><td>34</td><td>26</td></tr>
</table>

Table 15: Total number of Code breaches by size of institution

<table>
<tr><th></th><th colspan="2">2012–13</th><th colspan="2">2013–14</th><th colspan="2">2014–15</th><th colspan="2">2015–16</th></tr>
<tr><th></th><th>Total</th><th>Aver.[21]</th><th>Total</th><th>Aver.</th><th>Total</th><th>Aver.</th><th>Total</th><th>Aver.</th></tr>
<tr><td>Reported by all institutions</td><td>917</td><td>10.1</td><td>800</td><td>8.9</td><td>646</td><td>8.1</td><td>818</td><td>11.2</td></tr>
<tr><td>Reported by
- largest institutions</td><td rowspan="2">287</td><td rowspan="2">13.0</td><td rowspan="2">269</td><td rowspan="2">12.2</td><td rowspan="2">447</td><td rowspan="2">21.3</td><td>456</td><td>28.5</td></tr>
<tr><td>- large institutions</td><td>211</td><td>14.1</td></tr>
<tr><td>- medium institutions</td><td>520</td><td>18.6</td><td>455</td><td>16.3</td><td>119</td><td>4.8</td><td>49</td><td>3.1</td></tr>
<tr><td>- small institutions</td><td>110</td><td>2.7</td><td>76</td><td>1.9</td><td>80</td><td>2.4</td><td>102</td><td>3.9</td></tr>
</table>

Table 16: Number of institutions reporting Code breaches for period 2013–2015

	Number of institutions			
Number of self-reported Code breaches	**2012–13**	**2013–14**	**2014–15**	**2015–16**
Nil	35	39	31	24
Between 1 to 10	39	32	33	27
Between 11 to 20	7	10	5	8
Between 21 to 50	7	6	9	9
Between 51 to 100	2	1	2	5
Over 100	1	1	0	0

[20] Based on new definition of size of institution (see page 34).
[21] Average based on total number of Code breaches divided by number of institutions.

Table 17: Total number of customer complaints by size of institution

	2012–13		2013–14		2014–15		2015–16	
	Total	*Aver.*[22]	Total	*Aver.*	Total	*Aver.*	Total	*Aver.*
Reported by all institutions	14,393	*158.2*	12,409	*139.4*	16,709	*208.9*	14,100	*193.2*
Reported by[23] - largest institutions	11,292	*513.3*	9,732	*442.4*	14,107	*671.8*	11,215	*700.9*
- large institutions							1,815	*121.0*
- medium institutions	2,552	*91.1*	2,191	*78.2*	1,970	*78.8*	747	*46.7*
- small institutions	549	*13.4*	486	*12.5*	632	*18.6*	324	*12.5*

Table 18: Number of institutions reporting complaints for period 2013–2016

	Number of institutions			
Number of self- reported complaints	2012–13	2013–14	2014–15	2015–16
Nil	9	10	10	8
Between 1 to 10	23	29	18	19
Between 11 to 20	13	14	8	9
Between 21 to 50	18	10	17	11
Between 51 to 100	8	6	6	9
Between 101 to 1,000	17	18	18	13
Over 1,000	3	2	3	4

[22] Average based on total number of customer complaints divided by number of institutions.
[23] Based on new definition of size of institution (see page 34).