



**CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE**

ANNUAL COMPLIANCE REPORT 2016–17

A report on compliance with the Customer Owned Banking Code of Practice and the work of the Customer Owned Banking Code Compliance Committee.

December 2017

Contents

Chairman's message	4
Year at a glance.....	6
About the Code.....	7
Key promises.....	7
Code Compliance Committee.....	7
Committee meetings.....	8
Committee members.....	9
Code team staff	10
Code compliance monitoring.....	11
ACS program.....	11
Developing and improving the 2017 ACS.....	11
Self-reported Code breaches	11
Self-reported significant Code breaches	15
Code Subscribers' compliance initiatives	17
Internal dispute resolution	18
ACS Verification Program.....	25
Objectives.....	25
Scope	25
Findings.....	25
Investigations.....	27
Investigations registered in 2016–17	28
Own Motion Inquiries	30
Community engagement	30
Direct Debit Follow-Up.....	31
Engaging with stakeholders	32
Stakeholder liaison	32
Industry.....	32
Consumer advocates	32
Other.....	33
Publications.....	33
2017–18: Future outlook	34
Appendix A: Code Subscribers as at 30 June 2016	35
Appendix B: Comparative table of self-reported Code breaches	37
Appendix C: Additional tables – breach data by institution size	39
Appendix D: Significant self-reported Code breaches in 2016–17.....	41
Appendix E: Comparative table of self-reported complaints	43
Appendix F: Additional tables – complaints data by institution size	45
Appendix G: Additional tables – breach & complaints data	47
Appendix H: Definitions.....	48

About this report

This report assesses customer owned banking institutions' compliance with the 2016 Customer Owned Banking Code of Practice and covers the work undertaken by the Customer Owned Banking Code Compliance Committee from 1 July 2016 to 30 June 2017.

Data has been collated from monitoring the activities of the 67 institutions that subscribed to the Code in 2016–17, and consists of the outcomes of two Own Motion inquiries, the 2017 Annual Compliance Statement and Verification Program, and investigations into alleged Code breaches.

This document reports on the Committee's monitoring activities from 1 July 2016 to 30 June 2017, and shares the Committee's experience 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.

Chairman's message

By subscribing to the Customer Owned Banking Code of Practice, institutions express their commitment to fair and responsible banking. As the independent Committee responsible for monitoring compliance with the Code, the Code Compliance Committee focuses on assisting Code Subscribers to achieve this goal for the benefit of customers, institutions and the industry as a whole.

Breaches

This year, self-reported Code breaches increased once again, growing by almost half. Most institutions reported at least one breach, typically identified via internal audit and quality assurance processes, or from customer complaints. However, there are still a quarter of Code Subscribers – including large institutions – reporting no breaches of the Code.

Complaints

We welcomed improvement to Code Subscribers' reporting of complaints – this year there were fewer complaints not categorised by product or service. Our Annual Compliance Statement (ACS) enquiries also revealed that a large majority of Code Subscribers are recording details of the complaints they resolve within five days, exceeding their minimum legal reporting obligations.

Internal dispute resolution

Reversing a downward trend from last year, in 2016–17 institutions also reported an increase in customer complaints handled via their internal dispute resolution (IDR) processes. Most of these complaints were resolved in a timely way, most commonly by mutual agreement with the customer.

Benchmarking

The Committee's benchmarking data, included in this report, is a tool for institutions to assess where they stand in relation to others of a similar size. For those institutions keen to review and improve their processes for monitoring and reporting code breaches, initiatives of other Code Subscribers, described on page 25 of this report, may be a source of inspiration.

Privacy

In 2016–17, non-compliance with the Code's privacy obligations was once again the biggest source of self-reported Code breaches. Although associated customer complaints remain low, the inadvertent disclosure of personal information can have very serious consequences for customers. The Committee was pleased to see one institution respond to a spike in privacy breaches with a dedicated effort to review and improve compliance. We encourage other Code Subscribers seeing high levels of privacy breaches to adopt a similar approach.

The Committee would like to thank our Code team staff, particularly Sally Davis and Daniela Kirchlinde, for their dedicated service this year. We would also like to thank COBA and its former Chief Executive Officer, Mark Degotardi, as well as the many consumer advocates with whom we have engaged, for their support of our work in 2016–17.

At its heart, the Customer Owned Banking Code of Practice is a commitment by Code Subscribers to focus on proactively improving customer service. This means continuously reviewing and improving processes. Code Subscribers should be treating their breach and complaints registers not as something to simply fill out and file away, but as a valuable source of insight, learning and service improvement.

We look forward to working with all stakeholders to achieve this vision in 2017–18.

A handwritten signature in black ink, appearing to read "Sue-Anne Wallace". The signature is fluid and cursive, with a prominent initial "S" and a long, sweeping tail.

Dr Sue-Anne Wallace AM
Chairman
Customer Owned Banking Code Compliance Committee

Year at a glance

Compliance monitoring and breach reporting

1,216 breaches of the Code
self-reported by 51 (or 76% of) institutions (p. 11) **↑ from 818**

6 significant breaches of the Code
self-reported by 4 institutions (p. 15) **↓ from 11**

24% breaches of privacy obligations (D23)
self-reported by 34 (or 50% of) institutions (p. 14) **↓ from 30%**

12% breaches of responsible lending obligations (D6)
self-reported by 9 institutions (p. 14) **↑ from 3%**

18,662 IDR complaints
self-reported by 59 (or 88% of) of institutions (p. 18) **↑ from 14,100**

24% IDR complaints relating to customer service
self-reported by 42 (or 63% of) institutions (p. 21) **↓ from 31%**

90% of these IDR complaints
resolved within 21 days (p. 23) **↓ from 93%**



Own motion inquiry on community engagement (p. 30)



Own motion follow-up inquiry on direct debit (p. 31)

Investigations

4 new investigations matters received (p. 27)

22 individual compliance verification audits (p. 25)

Stakeholder engagement

23 stakeholder meetings (p. 32)

9 industry and consumer conferences presented to or attended (p. 32)

12 publications (p. 33)

About the Code

The 2014 Customer Owned Banking Code of Practice sets standards of good industry practice for the 67 institutions that have agreed to comply with its provisions when dealing with current and prospective individual and small business customers. By subscribing to the Code, customer owned banking 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.

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 10 key promises: general principles or values that apply to institutions’ dealings with all customers, as well as the broader community. Code Subscribers have committed to these 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

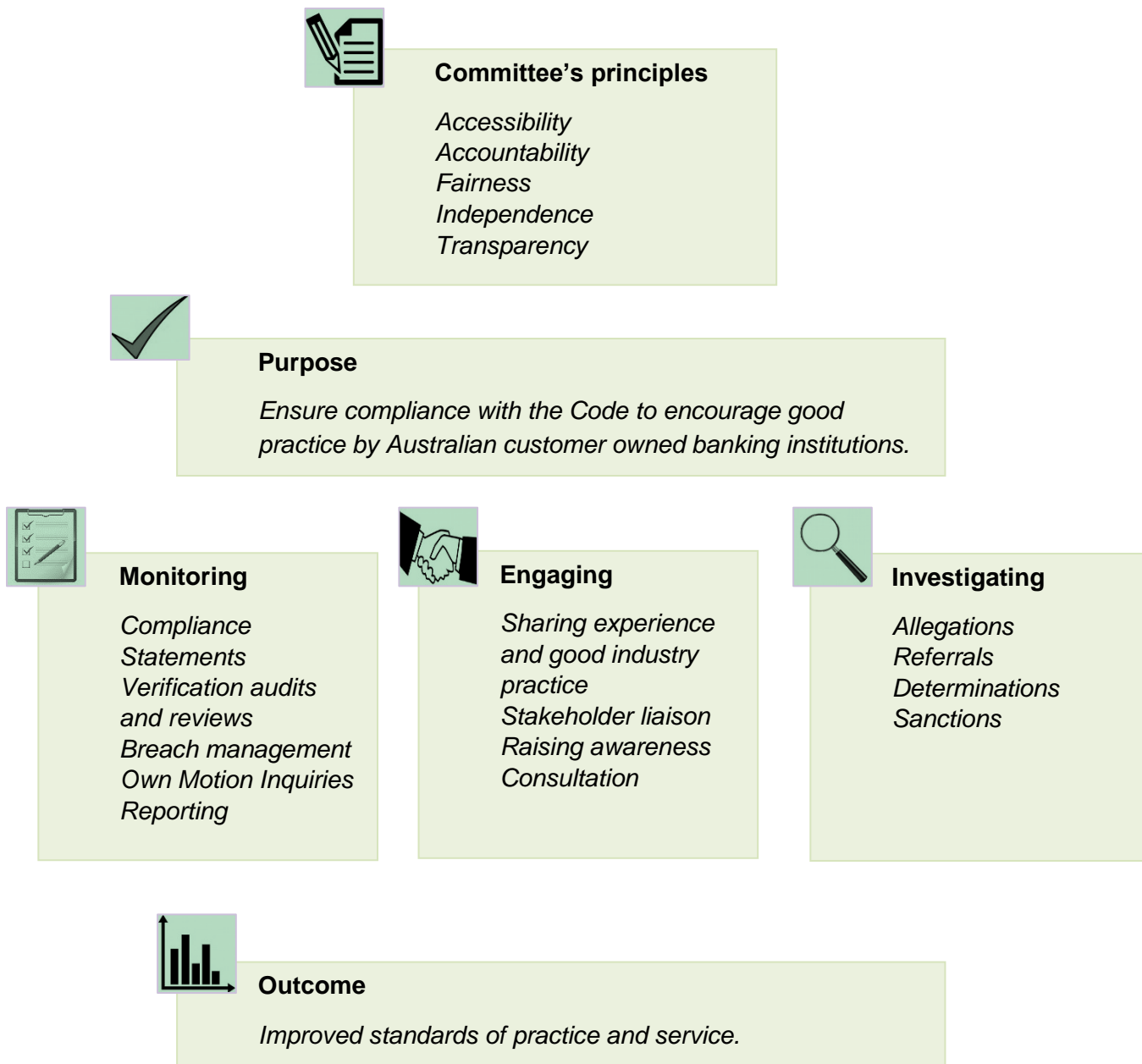
1. *We will be fair and ethical in our dealings with you.*
2. *We will focus on our customers.*
3. *We will give you clear information about our products and services.*
4. *We will be responsible lenders.*
5. *We will deliver high customer service and standards.*
6. *We will deal fairly with any complaints.*
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.*

Thirty specific sections detail how these key promises are to be delivered by Code Subscribers. Code Subscribers as at 30 June 2017 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 diagram below sets out the Committee’s purpose and principles, along with its key functions. These key functions can be grouped into three main categories: monitoring, investigating and engaging.



Committee meetings

In 2016–17, the Committee met formally five times. It also had informal individual meetings with the Code Team via telephone conferences, as well as meetings with COBA, regulators and other stakeholders. The Committee Chairman meets with the Chairman of COBA’s Board of Directors from time to time.

Committee members



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

Appointed: 18 February 2014¹
Term expires: 18 February 2019²

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

For the past 14 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.

In 2017, Sue-Anne was appointed as a Member of the Order of Australia (AM) for significant service to the not-for-profit sector, particularly through fundraising reform and codes of conduct.



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

Appointed: 1 January 2014
Term expires: 31 December 2019³

Anita is the Head of Legal, Governance and Compliance at Unity Bank and is the informal Chair and founder of the NSW Mutual Compliance Group. She has more than 20 years' experience working in compliance, including as Banking Compliance Manager for Citibank Australia, and has extensive broader financial services industry experience including lending, human resources and project management roles.

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



**Carolyn Bond AO
Consumer Representative**

Appointed: 1 March 2015
Term expires: 28 February 2020⁴

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.

Carolyn is currently contributing to industry policies which improve financial outcomes for victims of family violence. She is an Adjunct Professor at Deakin Business School and is a member of the Victorian Legal Services Board and the Financial Advisor Standards and Ethics Authority.

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 Re-appointed as at 18 February 2016, final term, not eligible for re-appointment.

³ Re-appointed as at 31 December 2016, final term, not eligible for re-appointment.

⁴ Re-appointed as at 28 February 2017, 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 (FOS) Australia in September 2015.

Sally previously worked as Senior Manager of Systemic Issues at FOS and has worked at FOS and its predecessor schemes for 17 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.

Her work as General Manager involves the oversight of four other codes of practice in the financial services industry in addition to the Customer Owned Banking Code of Practice.



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 21 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 compliance monitoring

The Committee's Code monitoring program gives customer owned banking institutions 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. In 2016–17, key Code monitoring activities were the 2017 Annual Compliance Statement (ACS) program and the ACS Verification Program.

ACS PROGRAM

The ACS is a self-assessment tool that helps Code Subscribers review their compliance with Code obligations. For Code Subscribers, completing the ACS is a core monitoring obligation, and includes self-reporting any Code breaches and complaints that are registered via the subscriber's IDR process. 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 2017 ACS

With the aim of achieving a consistent compliance monitoring approach, the 2017 ACS was reviewed and enhanced in partnership with COBA and a number of Code Subscribers. The ACS assessed:

- Code Subscribers' compliance with their Code obligations
- the robustness of their Code compliance monitoring frameworks
- the effectiveness of their compliance monitoring
- instances of non-compliance and how they were remedied
- emerging or significant compliance risks
- areas of good industry practice.

The ACS is completed and lodged via an online portal, which most Code Subscribers find effective. To assist Code Subscribers, the Committee provided a Frequently Asked Question document, Information Sheet and a sample showing how to lodge a breach and complaint. A newly developed webinar provided additional assistance. For the large majority of Code Subscribers (80%) completing ACS, including collecting the necessary data, took no more than two days.

Self-reported Code breaches

The ACS gathers two distinct breach data sets on '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 2016–17, Code Subscribers self-reported 1,216 Code breaches, an increase of 49% (398) on the 818 breaches reported in 2015–16. Around three quarters (76%) of Code Subscribers self-reported at least one breach of the Code, up from 68% in the previous reporting period. Around half (43%) of Code Subscribers reported between one and ten Code breaches.⁵ Just

⁵ See Appendix H, table 18 on page 48.

five large Code Subscribers collectively accounted for almost half (51% or 623) of the total of 1,216 Code breaches.

Most self-reported breaches were identified through quality assurance programs and internal audit processes. In addition, a fifth (242 or 20%) of breaches were identified as a result of customer complaint investigations, down from 31% 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

Covering the five years from 2012–13 to 2016–17, **Chart 1** shows the percentage of self-reported Code breaches that fell into each of the five broad categories of Code obligations.

Chart 1: Self-reported breaches by Code category, five years to 2016–17

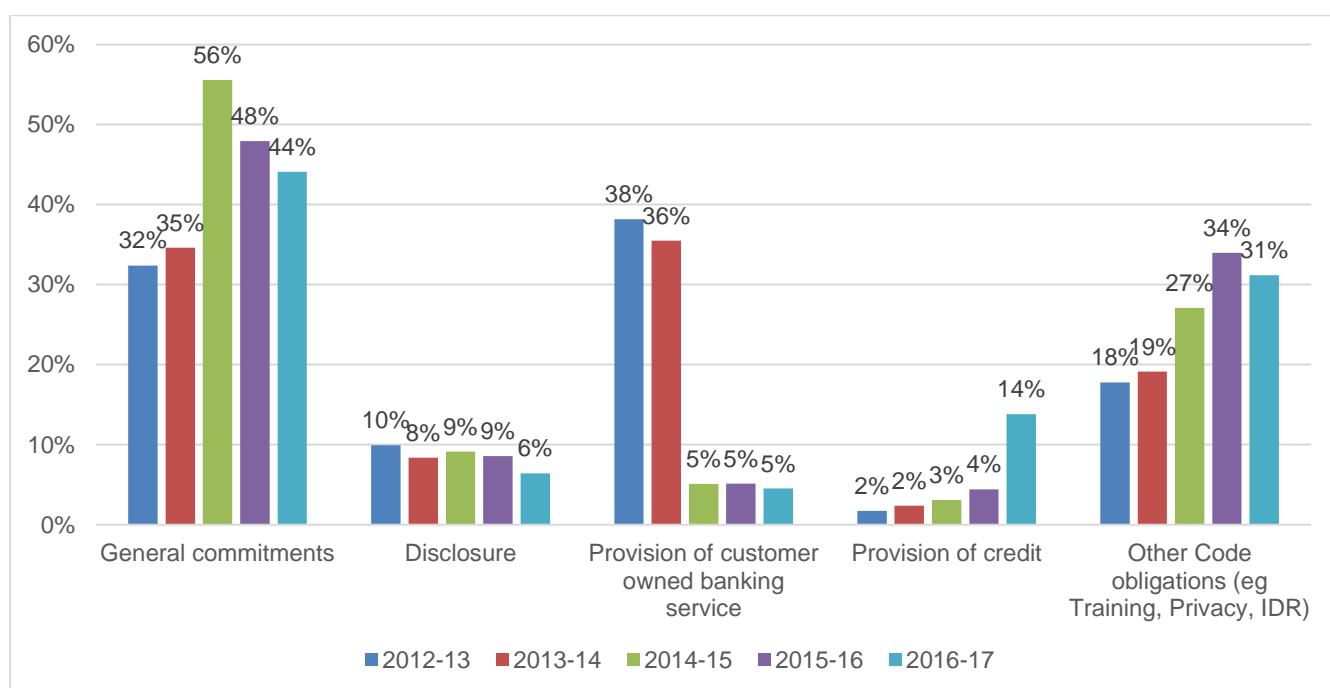


Chart 1 shows that the largest category of non-compliance in 2016–17 was ‘General commitments’, which comprised 44% of Code breaches. A further 31% of Code breaches were within the category of ‘Other’ obligations, comprising predominantly (24%) of non-compliance with privacy obligations.

Together, the two broad categories represented three-quarters (75%) of total Code breaches reported in 2016–17; slightly below the 2015–16 figure of 82%.

Table 2 provides greater detail, examining non-compliance with specific Code obligations over the same five-year period.

Table 2: Self-reported breaches by Code section, five years to 2016–17

	2012-13	2013-14	2014-15	2015-16	2016-17
General commitments	32%	35%	56%	48%	44%
Key commitments	31%	32%	49%	41%	35%
KP1 We will be fair and ethical in our dealings	0%	<1%	4%	<1%	<1%
KP2 We will focus on our customers	4%	3%	3%	3%	7%
KP5 We will deliver high customer service	18%	16%	25%	20%	6%
KP7 We will recognise our customers' rights	0%	0%	0%	<1%	11%
KP8 We will comply with our legal & industry obl.	9%	11%	17%	16%	11%
KP9 We will recognise impact on community	<1%	2%	0%	1%	<1%
Provision of general information	1%	3%	6%	7%	9%
KP3 We will give you clear information	0%	0%	0%	3%	2%
D2 Information about our products	1%	3%	5%	3%	7%
D19 Copies of documents, statements	0%	<1%	2%	<1%	<1%
Disclosure	10%	8%	9%	9%	6%
Interest rates, fees and charges	6%	8%	9%	7%	5%
D3 Information on interest rates, fees & charges	5%	8%	8%	6%	4%
D5 Reviewing fees and charges	1%	0%	1%	<1%	1%
T&C and changes to T&C (D4, D17)	4%	<1%	<1%	2%	1%
Provision of customer owned banking service	38%	36%	5%	5%	5%
Statement of accounts (D16)	1%	1%	3%	3%	2%
Direct debits arrangements (D20)	2%	1%	1%	<1%	1%
Chargebacks (D21)	16%	22%	0%	<1%	<1%
Recurring payment arrangements (D21.3)	<1%	<1%	<1%	<1%	0%
Closure of accounts (D22)	<1%	1%	<1%	<1%	<1%
Third party products (D13)	18%	11%	1%	1%	1%
Centrelink requirements (D26.5)	<1%	<1%	0%	0%	0%
Provision of credit	2%	2%	3%	4%	14%
Credit assessment (KP4, D6, D7, D24)	1%	2%	3%	4%	12%
Joint debtors, accounts and subsidiary cards (D9, D10, D11)	<1%	0%	0%	<1%	1%
Other provision of credit obligations (D8, D12, D26)	<1%	<1%	<1%	<1%	<1%
Other Code obligations (e.g. Training, Privacy, IDR)	18%	19%	27%	34%	31%
Privacy and confidentiality (D23)	12%	13%	20%	30%	24%
Advertising (D1)	1%	1%	2%	2%	2%
Communication (D15, D18, D25)	2%	3%	4%	1%	1%
Training (D14. E2)	<1%	1%	<1%	<1%	<1%
Dispute Resolution (KP6, D27, D28, D28, D30)	2%	1%	<1%	1%	3%
Promotion of the Code (B, KP10, E1)	1%	1%	0%	<1%	0%

Non-compliance with the privacy obligations in Section D23 of the Code was the most significant area of specific non-compliance in 2016–17, accounting for about one-quarter (24%) of self-reported breaches. Half of all institutions self-reported at least one breach of privacy obligations, with seven institutions reporting more than ten breaches each. Four large Code Subscribers accounted for nearly half (46%) of all privacy breaches, with one institution alone advising of 70 breaches.

Privacy

Privacy breaches commonly involved the advertent 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.

Responsible lending practice

Another main area of non-compliance was Section D6 of the Code, 'Responsible lending practices' representing 12% of total breaches. Nine Code Subscribers reported breaches in this area, with one large Code Subscriber alone reporting 86 breaches.

Customers' rights as owners and legal obligations

In addition, Key Promise 7 ('recognising customers' rights as owners') and Key Promise 8 ('compliance with legal and industry obligations') each contributed 11% of breaches in 2016–17. Compliance with legal and industry obligations also accounted for a substantial proportion of non-compliance in the previous year, whereas breaches of the obligation to recognise customers' rights as owners is a new area of concern. In the previous year only three breaches (less than one percent) and prior to that nil breaches were self-reported in this area. Key Promise 7 reflects the obligation to ensure that customers receive balanced and adequate information about the benefits, costs and impacts of any proposal to change the institution's ownership structure, such as mergers and takeovers.

High customer service and standards

Key Promise 5 ('delivery of high customer service and standards') has decreased in importance, contributing just 6% of breaches in 2016–17, down from 20% in the previous year. This may simply reflect changes to the ACS this year. In previous years, Key Promise 5 was listed repetitively throughout the compliance statement because it was seen as relevant to each breach category. This caused confusion and potential doubling up of breaches. In the 2016–17 ACS, therefore, it was only listed once, under the general commitments.

For a full comparative analysis of all self-reported Code breaches from 2012–13 to 2016–17, see [Appendix B](#), [Appendix C](#) and [Appendix H](#). For de-identified examples of Code breaches self-reported by Code Subscribers, including breach details and remedial actions, see [Appendix D](#).

Culture and framework of positive breach reporting

Sixteen Code Subscribers (24%) reported nil Code breaches in 2016–17. **Table 3** shows self-reported Code breach numbers by institution size⁶ in 2016–17.

⁶ For definitions of size of institutions, please see [Appendix H: Definitions](#)

Table 3: Self-reported Code breaches by institution size, 2016–17

Number of self-reported Code breaches	Micro institution	Small institution	Medium institution	Large institution	Total	Total 2015-16 for comparison
Nil	12	2	1	1	16	24
1 to 10	11	7	9	2	29	27
11 to 20	1	2	2	1	6	8
21 to 50	1	0	2	8	11	9
51 to 100	0	0	0	3	3	5
Over 100	0	0	0	2	2	0
Total	25	11	14	17	67	73

About half (48%) of micro institutions reported nil Code breaches. From the 17 large institutions, one reported nil Code breaches, while three-quarters (76% or 13) reported more than 20 breaches each.

Table 4 shows the self-reported Code breach mean for each institution size, which is provided for comparison and benchmarking purposes.

Table 4: Total and mean of self-reported Code breaches by institution size, 2016–17

	Micro institution	Small institution	Medium institution	Large institution	Total
Total number of self-reported Code breaches	2016–17	90	48	176	902
	2015–16	102	49	211	456
Mean per institution	2016–17	3.6	4.4	12.6	53.1
	2015–16	3.9	3.1	14.1	28.5

Over time, the Committee will use the collected data on self-reported Code breaches as a baseline for assessing trends. The data can also be used to benchmark an individual institution’s performance against other institutions of similar size. While there are many reasons why an institutions’ breach numbers might deviate from the average, this benchmarking might prompt an institution to review its compliance and/or monitoring processes.

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

As well as providing the above breach data, Code Subscribers also report on ‘significant breaches’ in the ACS. A **significant breach** of Code obligations is more serious than other breaches, as 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 Code compliance arrangements
- the extent of customer detriment

- remedial actions and costs incurred
- the duration of the breach.

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 also reported to ASIC. The role of the Committee is not to duplicate this regulatory action but to assist Code Subscribers to meet relevant Code obligations.

Four Code Subscribers – three large institutions and one micro – reported a total of six significant Code breaches in 2016–17. This is down from 11 significant Code breaches reported by seven Code Subscribers in 2015–16.

Table 5 shows the areas in which the significant Code breaches were recorded. Significant Code breaches in 2016–17 reflected different areas of concern to non-significant self-reported Code breaches. There were no significant breaches of privacy obligations.

Table 5: Self-reported significant breaches by Code section, five years to 2016–17

	2012– 13	2013– 14	2014– 15	2015– 16	2016– 17
General commitments	4	2	2	2	3
Key commitment (KP5 – high customer service)	0	0	0	0	1
Key commitment (KP7 – customers' rights)	0	0	0	0	1
Key commitment (KP8 – legal obligations)	3	2	1	2	0
Provision of general information (D2)	1	0	1	0	1
Disclosure	3	1	0	1	2
Interest rates, fees and charges (D3)	2	0	0	1	0
T&C and changes to T&C (D17)	1	1	0	0	2
Provision of credit	1	0	0	0	1
Credit assessment (KP4)	1	0	0	0	1
Provision of customer owned banking service	1	0	1	0	0
Statement of Accounts (D16)	1	0	1	0	0
Other Code obligations (e.g. Training, Privacy, IDR)	7	3	2	8	0
Advertising (D1)	1	1	0	2	0
Communication (D18)	0	1	0	0	0
Dispute Resolution (D28)	0	0	0	1	0
Privacy and confidentiality (D23)	1	1	2	5	0
Promotion of the Code (E1)	5	0	0	0	0
Total	16	6	5	11	6

Appendix E details 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 2016–17. These have strengthened compliance risk assessment processes and further embedded compliance requirements within institutions and across the industry.

Review of processes and procedures

Several Code Subscribers reviewed processes and procedures to improve compliance. For example, one Code Subscriber reviewed its processes in light of family violence issues. Other Code Subscribers described using the identification of Code breaches or Committee compliance activities to prompt efforts to improve compliance in specific areas, such as privacy and direct debit cancellation.

Adoption of new systems

To enable better monitoring and reporting, a number of Code Subscribers adopted new and better systems. For example, one Code Subscriber introduced a new Electronic Risk Management system with better capability for recording remedial action items, while another implemented a new Customer Relationship Management system that allowed for enhanced data extraction. Another Code Subscriber noted that its new incident reporting and management system greatly improved incident management, allowing all incidents to have Code breaches logged against them.

Improvement of existing processes and procedures

Many Code Subscribers reviewed and improved their monitoring processes and procedures. For example, some Code Subscribers introduced or extended attestation processes, while another focused on continual improvement to its branch audit processes. Several took steps to enhance complaints reporting. For example, one focused on more diligent complaints data entry; a second introduced quarterly complaints reviews to identify breaches; and a third centralised its process for reviewing customer feedback to ensure all issues were captured and reported upwards.

Staff training

Staff awareness was another area of improvement. Some Code Subscribers increased staff training on Code compliance or instituted new training in special areas, such as chargebacks, responsible lending or identifying Code incidents from customer complaints. Several Code Subscribers took steps to strengthen their compliance culture among staff, implementing measures such as monthly quizzes, regular sharing of complaint incidents among teams or focusing on encouraging staff to raise questions about compliance matters rather than waiting for audits.

Customer information

Some Code Subscribers also took steps to improve customer information. To improve their websites, Code Subscribers undertook comprehensive reviews or instituted regular website

checks, while others improved search functionality. One Code Subscriber took steps to make the Code available online and in branches, and another focused on ensuring that products were advertised in line with ASIC regulations.

Internal dispute resolution

The 2016–17 ACS collated data about Code Subscribers' 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

88% of Code Subscribers self-reported 18,662 complaints handled through their IDR process. This is a 32% increase from the 14,100 complaints reported in 2015–16.

Conversely, in its role as an external dispute resolution (EDR) provider, FOS reported that it accepted 126 disputes against 'credit unions' in 2016–17⁷. This is a 34% decrease from the 191 disputes reported in its previous review. Overall, disputes against 'credit unions' represent 0.5% of all disputes accepted by FOS.

The Credit & Investments Ombudsman (CIO) does not use the category 'credit unions'. Its 2016–17 Annual Report on Operations reports that 106 (1.8%) complaints were received against authorised deposit-taking institutions which include banks, mutual banks, building societies and credit unions.⁸ This is an increase on the 97 complaints reported relating to that category in its previous report.

Table 6 shows the number of self-reported complaints by size of institution.

Table 6: Self-reported IDR complaints by institution size, 2016–17

Number of self-reported IDR complaints	Micro institution	Small institution	Medium institution	Large institution	Total	Total 2015–16 for comparison
Nil	7	0	0	1	8	8
1 to 10	13	6	1	0	20	19
11 to 20	3	0	1	0	4	9
21 to 50	1	3	5	2	11	11
51 to 100	0	1	3	3	7	9
100 to 1,000	1	1	4	8	14	13
Over 1,000	0	0	0	3	3	4
Total	25	11	14	17	67	73

⁷ FOS Annual Review 2016-17, page 63.

⁸ CIO Annual Report on Operations 2016-17, page 48.

Only eight (12%) institutions did not self-report complaints; seven were micro institutions and one was a large institution. One-third of institutions reported more than 50 complaints each. Three large institutions reported more than 1,000 complaints.

For comparison and benchmarking purposes, **Table 7** provides the self-reported complaint average for institutions of different sizes. These figures are based on self-reported breach data. Institutions can draw comparisons with the mean number of self-reported complaints by institutions of similar size. Over time, the Committee will use this data to promote a culture and framework of positive complaints reporting.

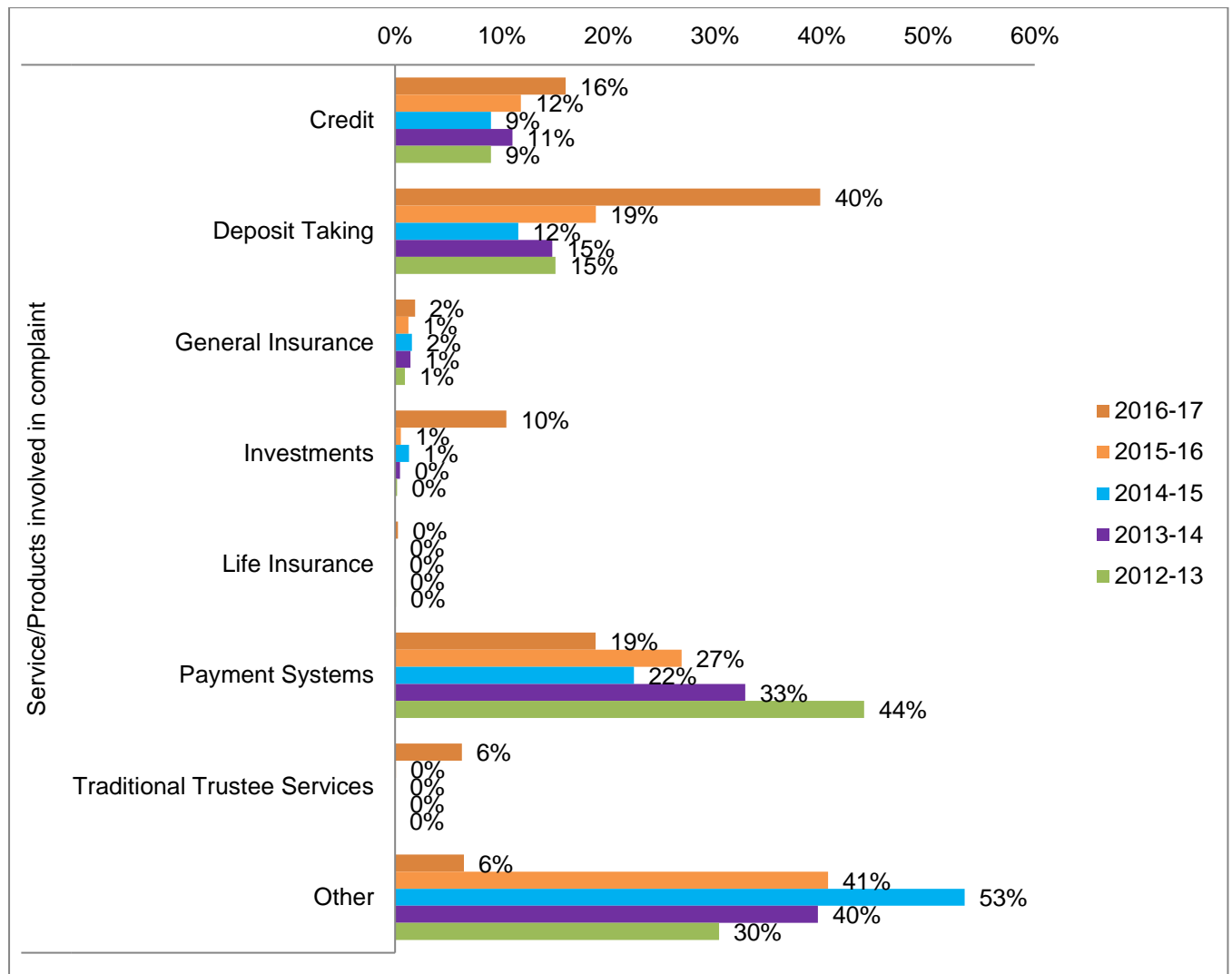
Table 7: Total and mean of self-reported IDR complaints by institution size, 2016-17

		Micro institution	Small institution	Medium institution	Large institution	Total
Total number of self-reported IDR complaints	2016–17	323	325	1,427	16,587	18,662
	2015–16	324	747	1,815	11,215	14,100
Mean per institution	2016–17	12.9	29.5	101.9	975.7	278.5
	2015–16	12.5	46.7	121.0	700.9	193.2

Complaint by service or product

Chart 2 shows the product or service involved in complaints that were handled via institutions' IDR processes. Most complaints related to deposit taking (40%), payment systems (19%) and credit products (12%). Only 6% of complaints were not categorised by product or service, a great improvement compared to the 41% in the 'Other' category in 2015–16. This may explain the increase in the categories 'Deposit Taking' and 'Investments'.

Chart 2: Self-reported IDR complaints by service or product, five years to 2016–17⁹



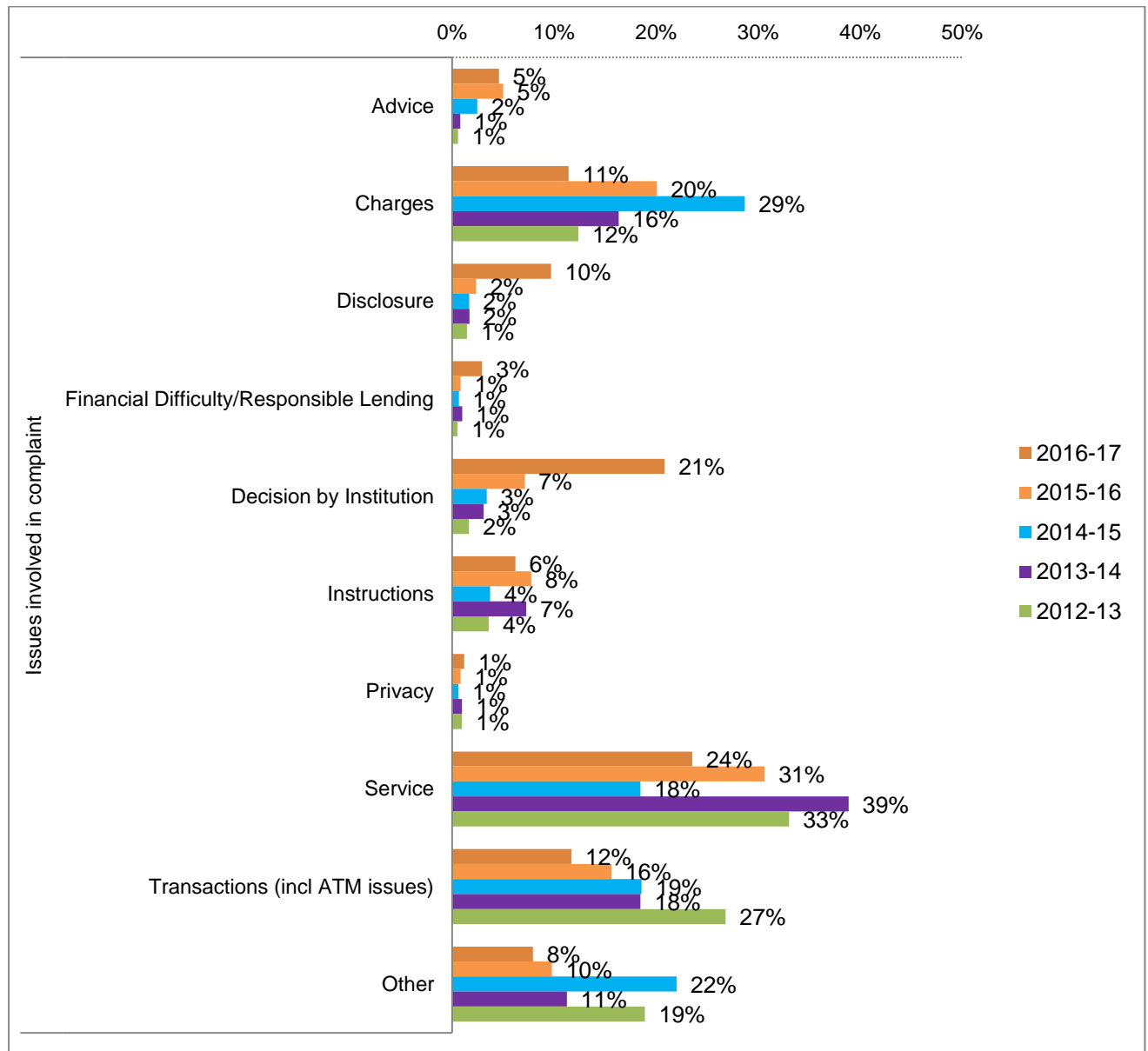
Complaint issues

Chart 3 shows that almost one in four complaints (24%) in 2016–17 related to service issues. One institutions' change to a new core banking system platform prompted complaints from customers who had difficulty with the associated change to customer and account numbers. Another institution reported that service-related complaints varied from outages due to a core banking system upgrade to the time taken to receive a cheque/deposit book by mail.

⁹ 'Other' represents the number of complaints that were noted by the institution, but not further identified regarding the service/product involved.

The other main complaint issues in 2016–17 were decisions made by the institution (21%); transactions, including ATM issues (12%); and charges (11%). Charges complaints often came from customers being dissatisfied with new fees, or seeking waivers for a fee incurred. Interestingly, the high number of self-reported breaches of privacy obligations was not reflected in complaints, of which only 1% concerned privacy.

Chart 3: Self-reported IDR complaints by issue, five years to 2016–17¹⁰

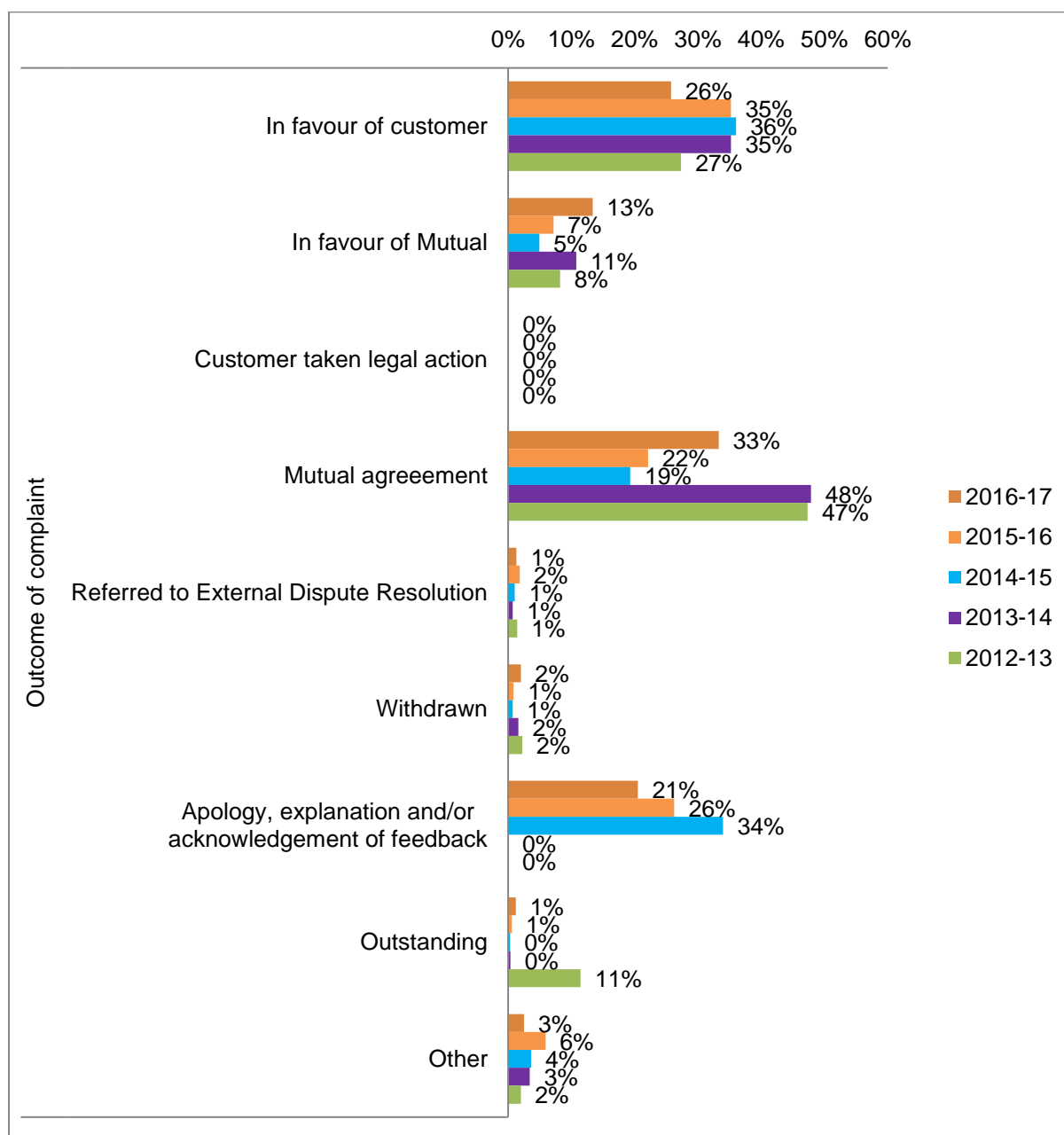


Complaint outcomes

Via the ACS, the Committee also collected information about how quickly and in what way institutions resolved complaints. **Chart 4** shows complaints by outcome for 2013–14 to 2016–17.

¹⁰ 'Other' represents the number of complaints that were noted by the institution, but not further identified regarding the issue involved.

Chart 4: Self-reported IDR complaints by outcome, five years to 2016–17¹¹



In 2016-17, around one in three complaints (33%) were resolved by mutual agreement and one in four complaints (26%) were resolved in favour of the customer. This is a change from 2015-16, where the majority of complaints (35%) were resolved in favour of the customer.

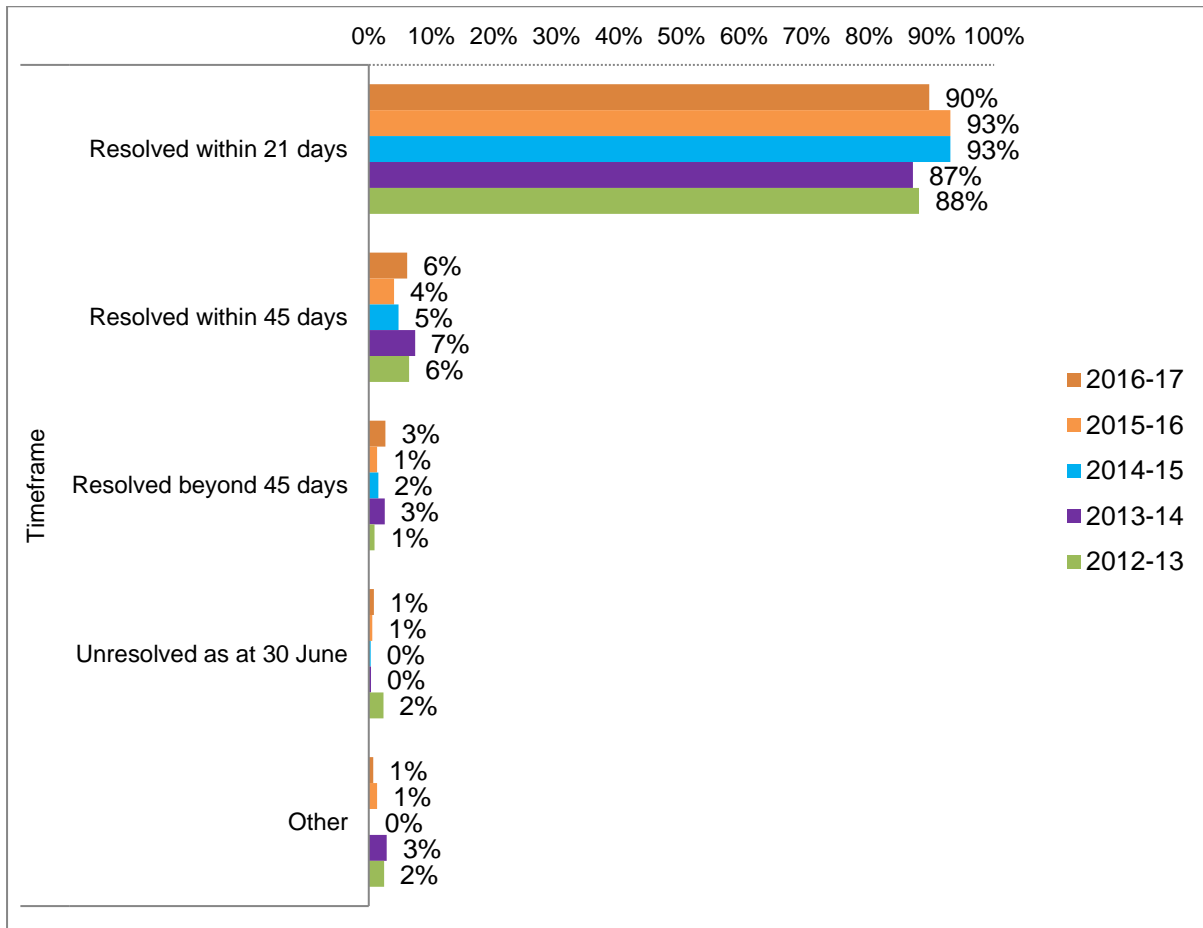
One Code Subscriber noted that resolution by mutual agreement typically involves a combination of solutions, such as fee waivers, the move to a more suitable product or service, explanations and apologies. A further one in five complaints (21%) were resolved with an apology or explanation of the situation to the customer.

¹¹ 'Other' represents the number of complaints that were noted by the institution, but not further identified regarding the outcome.

Complaint resolution timeframes

Chart 5 breaks down complaints by time taken to resolve.

Chart 5: Self-reported IDR complaints by resolution time, five years to 2016–17¹²



The majority of complaints (90%) were resolved within 21 days. Only 3% of customer complaints took longer than the required 45 days to resolve, in which case they were referred to the EDR provider.

This year, Code Subscribers were asked to comment on their reporting of complaints resolved within five business days. As these complaints do not have to be recorded under ASIC *Regulatory Guide 165.81* (RG 165.81),¹³ the Committee wanted to identify whether these complaints were recorded at all, and if so, what kind of information was recorded.

Commendably, 81% of institutions confirmed that they do record complaints that are resolved within five business days, exceeding the legislative requirement. Some Code

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

¹³ 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).

Subscribers noted, however, that they only record such complaints if they are major, or if they remain unresolved on first contact and need to be escalated.

Table 8 shows the relationship between institution size and the reporting of complaints resolved within five business days.

Table 8: Recording of IDR complaints resolved within five business days by institution size

<i>Do you record complaints resolved 'within five business days'?</i>				
<i>Size of institution</i>	Yes		No	
Micro institution	20	80%	5	20%
Small institution	8	73%	3	27%
Medium institution	13	93%	1	7%
Large institution	13	76%	4	24%
Total	54	81%	13	19%

Table 9 shows the relationship between institution size and the reporting of specific details on these complaints such as the product, issue and outcome. Those institutions that do record details typically commented that they record the same details for all complaints, regardless of resolution timeframe.

Table 9: Recording of detailed information about complaints resolved within five business days by institution size

<i>Do you record detailed information regarding complaints resolved 'within five business days'?</i>				
<i>Size of institution</i>	Yes		No	
Micro institution	22	88%	3	12%
Small institution	8	73%	3	27%
Medium institution	12	86%	2	14%
Large institution	11	65%	6	35%
Total	53	79%	14	21%

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 customers first. In addition to quantitative data, most Code Subscribers provided valuable comments and information about complaints.

For a full comparative analysis table of all self-reported complaints data from 2013–14 to 2016–17, see [Appendix F](#), [Appendix G](#) and [Appendix H](#).

ACS 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

The objectives of the ACS Verification Program were to:

- discuss any specific non-compliance issues that were reported in the 2016 ACS for the previous period (1 July 2015 to 30 June 2016)
- assist the Committee to understand how institutions manage and monitor their compliance with the Code, and
- share examples of good industry practice.

Scope

The ACS Verification Program was conducted via teleconference between November and early December 2016. Twenty-two institutions participated, including all institutions with over \$1b assets and five other institutions varying in size, as shown in **Table 10** below.

Table 10: Institutions participating in the 2016 ACS Verification Program

Size of institution	ACT	NSW	Qld	SA	Vic	WA	Total
Large institution	1	8	4	1	3	1	18
Medium institution		1					1
Small institution		1					1
Micro institution		1	1				2
Total	1	11	5	1	3	1	22

Before each teleconference, institutions were provided with a copy of their 2015–16 ACS response and, for the first time, with an 'Aggregated Outcomes and Comparative Data' document. This newly-developed comparative data document provides more targeted feedback so that institutions can benchmark their compliance outcomes against industry performance in general and against other institutions of the same size. The document detailed aggregated self-reported breach activity; high-level Code compliance trends over five years; and the institution's breach and complaint numbers benchmarked against other institutions of the same size.

Findings

From the ACS Verification Program, the Committee generated findings about compliance frameworks, Code breach data sources, and inconsistencies in how institutions self-report on complaints.

Inconsistent self-reporting of complaints data

One of the biggest challenges in the ACS is inconsistency in how institutions report complaints. Reasons for inconsistency are varied. Most of those institutions that do not self-report matters resolved on the spot or within five business days cited internal inconsistent reporting and lack of system capabilities.

Participating institutions acknowledged that the current ACS data is a good starting point, but raised concerns about the integrity of the data, and questioned whether the comparative data allows for accurate comparisons.

As a result, the Committee agreed to continue to collect complaints data for matters resolved on the spot and matters resolved within five business days, but record it separately in the 2017 ACS (not as part of the timeframe for complaints). It will also review the comparative complaints data.

Positive compliance culture

The level of maturity and sophistication of an institution's compliance framework often depends on the systems and infrastructure that support the framework. The ACS Verification Program showed that institutions are moving towards a compliance culture of transparency and 'no blame' approach, which the Committee encourages.

Identifying Code breaches

The majority of participating institutions confirmed that complaints registers are the only source for identifying Code breaches. Institutions need to look beyond their complaints data for sources to identify Code breaches and to promote a positive compliance culture, including:

- review of policies, procedures and products
- internal staff referrals and internal audits/compliance reviews
- monitoring and quality assurance programs
- feedback from third parties, and
- external audits.

Investigations

The Charter¹⁴ and the Code empower 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 10: How to respond to a review of an alleged Code breach

Following a review of an alleged Code breach, the Committee expects institutions to:

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

¹⁴ The Charter governs the relationship between the Committee and the COBA Board. Together with the Code, it sets out the terms under which the Committee operates, for the purpose of exercising its powers, functions and duties.

INVESTIGATIONS REGISTERED IN 2016–17

In 2016–17 the Committee received four new matters for investigation: one from a financial counsellor, one from a consumer advocate and two directly from customers. The subsequent assessments are summarised in **Table 11** according to the Code sections considered in each case.

Table 11: Investigations registered in 2016–17

<p>D20.1 – Cancellation of direct debit arrangements</p>	<p>Issue</p> <p>This issue was referred to the Committee by a consumer advocate, who noted that the Terms and Conditions (T&Cs) on the institution’s website did not comply with obligations under the Code regarding cancellation of direct debit arrangements. In particular, the T&Cs stated that the customer must contact the biller before contacting the institution. This had already been highlighted to the institution following an Own Motion in 2010.</p> <p>Outcome</p> <p>In May 2017, the institution noted the compliance issue in their response to the Committee’s Own Motion inquiry on direct debit. It confirmed that the wording would be rectified in the next T&C document update (scheduled for October 2017) to note that the customer is not required to contact the biller first to cancel a direct debit arrangement.</p> <p>Status</p> <p>Closed – Code breach.</p>
<p>D1 – Advertising D13 – Third party products and services</p>	<p>Issue</p> <p>The complainant made a purchase on his credit card relating to overseas travel and then received travel marketing material about travel insurance via email. The complainant already had travel insurance as part of his credit card bundle. The complainant was concerned that he had travel insurance already bundled with his credit card, but there was no reminder about this in the marketing material. Since some consumers have limited knowledge about travel insurance bundled with credit cards, the complainant was concerned that there is a real chance that institutions are encouraging someone to purchase insurance to cover a risk that is already covered.</p> <p>Outcome</p> <p>The matter has been discussed and assessed with the complainant and the institution. It was agreed that it would be more appropriate to address this area separately.</p> <p>Status</p> <p>Closed – no individual investigation undertaken.</p>

<p>D19 – Copies of documents, statements and other information</p> <p>D26 Debt collection</p>	<p>Issue</p> <p>The complainant alleged in a telephone call that the institution involved sold his property without his consent and ‘through conspiracy and fraud’ and did not respond to his request to provide information regarding the alleged debt.</p> <p>Outcome</p> <p>Despite various follow up attempts, the complainant did not provide any further written information regarding his allegation or a privacy authority form.</p> <p>Status</p> <p>Closed – unable to proceed due to lack of information.</p>
<p>D13 – Third party products and services</p>	<p>Issue</p> <p>A financial counsellor raised questions about her user/consumer experience while being offered gap insurance by an institution in relation to a car loan.</p> <p>Outcome</p> <p>It was confirmed that the financial counsellor only wanted to clarify that there were two contracts – one for the insurance and one for the loan. In general, she confirmed that the institution involved was very helpful and informative regarding the sale of the gap insurance. There was no complaint or issue.</p> <p>Status</p> <p>Closed – enquiry only.</p>

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 promote improvement in 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 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 the report did not address specific areas of Code non-compliance, but examined how institutions ensure compliance.

To ensure continuing effective community engagement by customer owned banking institutions, the Committee encourages institutions to:

- regularly review the definition of community to ensure that it includes the wider community as well as the community represented by the institution's customers and staff
- review how communities are defined to ensure that the institution's community engagement programs deliver sustainable impact for community benefit
- ensure community engagement methods promote and contribute to the community served and are not designed mainly for promotion and commercial gain
- match the focus and products of the institution's community engagement to the special needs and concerns of the communities served
- embrace social media to offer a range of communication channels adapted to the characteristics of the communities served
- put robust measurements in place regarding the impact of the institution's community engagement to ensure effectiveness

- continue to add value and credibility to the institution's engagement policy by including it in the Business Plan and Annual Budget
- consider how community engagement is reported in the institution's publications including the Annual Report.

The [full report](#) was published in January 2017 and can be found on the Committee website¹⁵.

DIRECT DEBIT FOLLOW-UP

In May 2017, the Committee conducted a follow-up OMI into institutions' compliance with the direct debit obligations in section 20.1 of the Code.

'We will act promptly to cancel a direct debit facility linked to your transaction account if you ask us to do so, and we will give you an estimate of how long cancellation will take. We will not tell you to try and cancel the facility with the biller or other direct debit user first (but we may suggest that you also contact the direct debit user).'

The ability for customers to cancel direct debits via their institution is a powerful safeguard, especially for customers who are in financial difficulty. Failure for institutions to accept or act on notice of a direct debit cancellation request may cause members who are already in financial trouble to be further impacted when fees are imposed on the account.

The findings from previous inquiries, in 2010 and 2012, were disappointing, and did not meet the Committee's expectations. More recently, institutions have self-reported minimal breaches of their direct debit obligations. In 2015–16, institutions self-reported three breaches of these obligations, fewer than the 15 breaches self-reported in the 2012–13. It is unclear whether the reduced breach numbers reflect an improvement in the industry's compliance performance or a lack of monitoring by institutions in this area.

Information for the inquiry was collected using an online questionnaire, completed by 66 institutions, and by auditing 17 large institutions' websites. A report on the findings will be published in 2017–18¹⁶. The Committee is also planning a further follow-up as part of the next ACS to check if institutions have implemented the recommendations in this forthcoming report.

¹⁵ See <http://www.cobccc.org.au/uploads/2017/01/COB-OMI-Community-Engagement-18Jan2017.pdf>

¹⁶ See <http://www.cobccc.org.au/uploads/2017/09/COB-OMI-Direct-Debit-Follow-Up-Sep2017.pdf>

Engaging with stakeholders

In 2016–17, in addition to engaging with Code Subscribers the Committee continued to engage with stakeholders to influence positive changes in industry behaviour, share its experience of Code compliance and highlight areas of good industry practice.

STAKEHOLDER LIAISON

Throughout 2016-17, 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 Chairman met regularly with the COBA Board Chairman, Wendy Machin, following each Committee meeting. The General Manager had regular meetings with former COBA CEO, Mark Degotardi. The General Manager and the Committee's Industry Representative presented on Code matters at the COBA Board meeting in April 2017.

The Committee's Chairman and Industry Representative, as well as the General Manager attended COBA's convention in Adelaide. The Committee's Chairman and General Manager also interacted with industry at the FOS Conference in Melbourne and at the Credit Law Conference in Queensland in September 2016. The General Manager also presented at the March 2017 Responsible Lending and Borrowing Summit in Sydney.

Through these meetings the Committee ensured that the Board and industry association generally continued to be aware of the Committee activities. It also provided an opportunity for feedback about current industry issues.

Consumer advocates

Engagement with the financial counselling sector was a focus throughout 2016–17. The General Manager met with Financial and Consumer Rights Council (FCRC) Executive Officer, Peter Gartlan, and Fiona Guthrie, CEO of Financial Counselling Australia (FCA).

In addition, the Compliance Manager presented at the Money Workers Association of the Northern Territory Conference in Darwin in November 2016, and attended the following financial counselling sector conferences:

- Financial and Consumer Rights Council Conference in Melbourne (September 2016)
- Financial Counsellors' Association of NSW Conference in Sydney (September 2016)
- Financial Counsellors' Association of Queensland Annual State Conference in Port Douglas (March 2017)
- Financial Counselling Australia Conference 'Making waves' on the Gold Coast (May 2017).

Consumer advocates attended a Melbourne meeting with Committee members in October 2016. In November 2016, the Compliance Manager engaged with and trained consumer

advocates alongside the Consumer Action Law Centre and WEstjustice¹⁷ at sessions in Melbourne and Werribee. The same month in Queensland, the Compliance Manager met with Queensland Legal Aid.

Finally, the Compliance Manager participated in the August 2016 NAIDOC¹⁸ week launch of the FOS Reconciliation Action Plan.

Attendance at these conferences and face to face meetings with consumer advocates assist the Committee in understanding common issues that affect consumers regarding banking products and services. This informs the Committee's risk analysis and targeted monitoring framework. At the same time, consumer advocates are kept informed about the Committee's work and the ability to advise it of possible issues that are covered by the Code.

Other

The General Manager engaged with relevant ombudsman schemes. As well as exchanging information with FOS on EDR issues, the General Manager met with the Credit and Investments Ombudsman. In August 2016, the General Manager also met with the Deputy Commissioner at the Office of the Australian Small Business Commissioner, Craig Latham.

Regular meetings with ASIC were also held, and the Committee and General Manager participated in the ASIC Annual Forum in March 2017.

The General Manager facilitated joint meetings for the four code committees (insurance brokers, general insurance, banking and customer owned banking) serviced by the Code team. Following a meeting for all independent chairmen of these committees in September 2016, a separate meeting of consumer representatives was held in October 2016. These meetings are a valuable forum in which to discuss, share and compare compliance monitoring issues among the various financial services industry sectors.

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.

During 2016–17, the Committee published:

- four articles in *The Circular*, FOS's online magazine (editions 26, 27, 28 and 29)
- information about code monitoring committees in the FCRC newsletter *Devil's Advocate*
- a Code e-learning module for external stakeholders
- three editions of the *Accomplish* e-newsletter, keeping stakeholders up-to-date with activities and Code compliance news (editions 28–30)
- a report on the *Own Motion Inquiry 'Community Engagement'* (January 2017).

¹⁷ Formed through a merger of the Footscray Community Legal Centre, Western Suburbs Legal Service and Wyndham Legal Service.

¹⁸ National Aborigines and Islanders Day Observance Committee.

2017–18: Future outlook

The Committee's primary objectives for 2017–18 are to:

- improve interaction and engagement with Code Subscribers, consumer advocates and regulators
- review and improve analytical work in risk based areas to ensure compliance with Code obligations, and
- ensure a collaborative approach to encourage good industry practice.

Following the publication of the Own Motion follow-up Inquiry on Direct Debits, a new major Own Motion Inquiry concerning privacy obligations is planned for the first quarter of 2017–18. This is an area of emerging industry risk identified through analysis of ACS results.

Based on the analysis of the 2017 ACS data, around 10% of Code Subscribers (including all those with more than \$1b in assets) will participate in the ACS Compliance Verification program in the second quarter of 2017–18. Each participant will receive an individual benchmarking document outlining their comparative breach and complaints data.

In the final quarter of 2017–18, the 2018 ACS program will ask Code Subscribers again to self-report complaints and breach data for the period 1 July 2017 to 30 June 2018.

We will continue our focus on engagement and communication, working with COBA, industry cluster groups, consumer advocates and Code Subscribers to promote understanding of the Committee's operations, and encourage positive breach and complaints monitoring and reporting.

The Committee may also engage in the upcoming COBA Code review; the proposed new one-stop-shop EDR scheme including the transition from FOS to the Australian Financial Complaints Authority (AFCA); and the Australian Treasury proposal to make all financial industry codes mandatory and approved by ASIC.

Appendix A: Code Subscribers

as at 30 June 2017

Australian Central Credit Union Ltd t/as People's Choice Credit Union	mecu Limited t/as Bank Australia
Big Sky Building Society Ltd	t/as Intech Bank
Broken Hill Community Credit Union Ltd	Members Banking Group Limited
CAPE Credit Union Ltd	t/as RACQ Bank
Capricornian Ltd	My Credit Union Limited
Central Coast Credit Union t/as Wyong Shire Credit Union Ltd	Northern Inland Credit Union Ltd
Central Murray Credit Union Ltd	Nova Credit Union Limited
Central West Credit Union Limited	Orange Credit Union Limited
Coastline Credit Union Ltd	Police and Nurses Limited
Community Alliance Credit Union Limited t/as Catalyst Money	t/as P&N Bank
t/as Illawara Credit Union	Police Bank Ltd
t/as Western City Credit Union	t/as Police Bank
Community CPS Australia Limited	t/as Customs Bank
t/as Beyond Bank	Police Credit Union Limited
Community First Credit Union Limited	Pulse Credit Union Ltd
t/as Northern Beaches Credit Union	t/as Pulse Credit Union
Community Mutual Ltd	t/as La Trobe University Credit Union
t/as Hunter Mutual	t/as Melbourne University Credit Union
t/as New England Mutual	QPCU Limited
t/as Orana Mutual	t/as QBANK
t/as Regional Australia Bank	Quay Credit Union Ltd
Credit Union Australia Ltd	Qudos Mutual Limited
t/as CUA	t/as Qudos Bank
Credit Union SA Limited	Queensland Country Credit Union Limited
Dnister Ukrainian Credit Co-Operative Ltd	ECU Australia
EECU Limited	Queenslanders Credit Union Limited
t/as Nexus Mutual	Railways Credit Union Ltd
Family First Credit Union Limited	t/as MOVE People Driven Banking
Fire Service Credit Union Ltd	t/as myMOVE
Firefighters & Affiliates Credit Co-operative Limited t/as Firefighters Credit Union	Select Encompass Credit Union Limited
First Choice Credit Union Ltd	SGE Mutual Limited
First Option Credit Union Limited	t/as G&C Mutual Bank
Ford Co-operative Credit Society Limited	South West Credit Union Co-operative Ltd
Gateway Credit Union Ltd	South West Slopes Credit Union Ltd
Goulburn Murray Credit Union Co-Operative Ltd	Southern Cross Credit Union Ltd
Greater Bank	Summerland Credit Union Limited
Heritage Bank Limited	Sydney Credit Union Ltd
Heritage Isle Credit Union Ltd	t/as Comtax Credit Union
Holiday Coast Credit Union Ltd	Teachers Mutual Bank Limited
Horizon Credit Union Ltd	t/as Teachers Mutual Bank
Hume Bank Limited	t/as UniBank
Laboratories Credit Union Limited	t/as Firefighters Mutual Bank
Lysaght Credit Union Ltd	Traditional Credit Union Ltd
Macarthur Credit Union Ltd	Transport Mutual Credit Union Ltd
t/as The Mac	Unity Bank
Macquarie Credit Union Ltd	t/as Unity Bank Limited
Maitland Mutual Building Society Ltd	t/as Bankstown City Unity Bank
t/as The Mutual	t/as Reliance Bank
MCU Limited	Victoria Teachers Limited
t/as Maleny Credit Union	t/as Victoria Teachers Mutual Bank
	Warwick Credit Union Ltd
	WAW Credit Union Co-operative Ltd
	Woolworths Employees Credit Union Limited

Table 12: Code Subscribers by state (head office) and size of institution¹⁹

As at 30 June 2017	NSW	NT	QLD	SA	TAS	VIC	WA	Total	Comparison to 2015-16
Large institutions	9	-	4	1	-	2	1	17	16
Medium institutions	9	-	2	2	-	1	-	14	15
Small institutions	6	-	3	-	-	2	-	11	16
Micro institutions	12	1	1	2	1	8	-	25	26
Total	36	1	10	5	1	13	1	67	73
<i>Comparison to 2015-16</i>	40	1	11	5	1	14	1	73	
<i>Comparison to 2014-15</i>	44	1	12	5	1	16	1	80	

¹⁹ Institutions are counted by Australian Financial Service License.

Appendix B: Comparative table of self-reported Code breaches

Table 13: Number of self-recorded breaches by Code category and section

	2012-13		2013-14		2014-15		2015-16		2016-17	
	Total	Sig	Total	Sig	Total	Sig	Total	Sig	Total	Sig
General commitments	297	4	277	2	359	2	392	2	536	3
Key commitments	287	3	256	2	318	1	338	2	426	2
KP1 Be fair and ethical	0	0	2	0	26	0	3	0	4	0
KP2 Focus on our customers	41	0	21	0	20	0	27	0	84	0
KP5 Deliver high customer service	166	0	127	0	162	0	166	0	69	1
KP7 Recognise our customers' rights	0	0	0	0	0	0	3	0	129	0
KP8 Comply with legal & ind. obligations	79	3	89	2	110	1	130	2	138	0
KP9 Recognise impact on community	1	0	17	0	0	0	9	0	2	1
Provision of general information	10	1	21	0	41	1	54	0	110	1
KP3 Clear information	10	1	2	0	0	0	27	0	24	0
D2 product information	0	0	18	0	31	1	23	0	80	1
D19 copies of documents	0	0	1	0	10	0	4	0	6	0
Disclosure	91	3	67	1	59	0	70	1	78	2
Interest rates, fees and charges	56	2	65	0	57	0	54	1	61	0
D3 Interest rates, fees and charges	50	2	65	0	49	0	53	1	45	0
D5 Reviewing fees and charges	6	0	0	0	8	0	1	0	16	0
T&C and changes to T&C	35	1	2	1	2	0	16	0	17	2
D4 Fair terms and conditions	25	0	0	0	0	0	11	0	2	0
D17 Notifying changes to your account	10	1	2	1	2	0	5	0	15	2
Provision of customer owned banking service	350	1	284	0	33	1	42	0	55	0
D13 Third party products	166	0	84	0	4	0	9	0	14	0
D16 Statement of accounts	13	1	11	0	21	1	23	0	27	0
D20 Direct debit arrangements	15	0	9	0	4	0	3	0	7	0
D21 Chargebacks	151	0	172	0	0	0	4	0	2	0
D21.3 Recurring payment arrangements	2	0	3	0	3	0	2	0	0	0
D22 Closure of accounts	2	0	4	0	1	0	1	0	5	0
D26.5 Centrelink requirements	1	0	1	0	0	0	0	0	0	0
Provision of credit	16	1	19	0	20	0	36	0	168	1
Credit assessment, responsible lending and financial difficulty	11	1	16	0	18	0	32	0	151	1
KP4 We will be responsible lenders	3	1	4	0	2	0	8	0	6	1
D6 Responsible lending practices	6	0	9	0	15	0	20	0	143	0

	2012-13		2013-14		2014-15		2015-16		2016-17	
	Total	Sig	Total	Sig	Total	Sig	Total	Sig	Total	Sig
D7 Credit limit increase offers	0	0	0	0	0	0	1	0	0	0
D24 If you are in financial difficulties	2	0	3	0	1	0	3	0	2	0
Joint debtors, accounts & sub. cards	1	0	0	0	0	0	1	0	11	0
D9 Joint accounts	1	0	0	0	0	0	0	0	9	0
D10 Subsidiary cards	0	0	0	0	0	0	0	0	2	0
D11 Safeguards for co-borrowers	0	0	0	0	0	0	1	0	0	0
Other provision of credit obligations	4	0	3	0	2	0	3	0	6	0
D8 Reverse mortgage loans	0	0	0	0	0	0	0	0	0	0
D12 Safeguard for loan guarantors	2	0	0	0	1	0	2	0	2	0
D26 Debt collection and legal action	2	0	3	0	1	0	1	0	4	0
Other Code obligations (such as Training, Privacy, IDR)	163	7	153	3	175	2	278	8	379	0
Privacy and confidentiality	111	1	105	1	129	2	244	5	294	0
D23 Information privacy and security	111	1	105	1	129	2	244	5	294	0
Advertising	7	1	10	1	13	0	17	2	21	0
D1 Advertising	7	1	10	1	13	0	17	2	21	0
Communication	21	0	23	1	27	0	7	0	18	0
D15 Timely, clear and effective	12	0	20	0	21	0	4	0	15	0
D18 Electronically	9	0	2	1	6	0	3	0	3	0
D25 Working with your representative	0	0	1	0	0	0	0	0	0	0
Training	4	0	5	0	3	0	4	0	5	0
D14 Use of finance brokers	0	0	0	0	0	0	0	0	0	0
E2 Training our staff	4	0	5	0	3	0	4	0	5	0
Dispute Resolution	15	0	5	0	3	0	5	1	41	0
KP6 Deal fairly with any complaints	6	0	0	0	0	0	0	0	0	0
D27 Prompt, fair resolution of complaints	4	0	3	0	0	0	5	0	39	0
D28 Our complaints handling process	5	0	1	0	2	0	0	1	1	0
D29 External Dispute Resolution (EDR)	0	0	1	0	1	0	0	0	1	0
D30 Complaints about Code breaches	0	0	0	0	0	0	0	0	0	0
Promotion of the Code	5	5	5	0	0	0	1	0	0	0
B Commitment to comply with Code	3	1	0	0	0	0	0	0	0	0
KP10 Support and promote Code	1	0	0	0	0	0	1	0	0	0
E1 Publicising the Code	1	4	5	0	0	0	0	0	0	0
Grand Total	917	16	800	6	646	5	818	11	1,216	6

Appendix C: Additional tables – breach data by institution size

Table 14: Number of self-reported breaches within each Code category by size of Code Subscriber in 2016-17

Service Standards	Micro institution	Small institution	Medium institution	Large institution	Total
General commitments	39	23	405	69	536
Key commitments	34	23	309	60	426
KP1 Be fair and ethical	0	0	4	0	4
KP2 Focus on our customers	3	3	64	14	84
KP5 Deliver high customer service	30	1	16	22	69
KP7 Recognise our customers' rights	0	0	125	4	129
KP8 Comply with legal & ind. obligations	1	19	98	20	138
KP9 Recognise impact on community	0	0	2	0	2
Provision of general information	5	0	96	9	110
KP3 Clear information	1	0	20	3	24
D2 product information	4	0	74	2	80
D19 copies of documents	0	0	2	4	6
Disclosure	19	4	37	18	78
Interest rates, fees and charges	12	4	31	14	61
D3 Interest rates, fees and charges	3	3	29	10	45
D5 Reviewing fees and charges	9	1	2	4	16
T&C and changes to T&C	7	0	6	4	17
D4 Fair terms and conditions	0	0	0	2	2
D17 Notifying changes to your account	7	0	6	2	15
Provision of customer owned banking service	11	0	33	11	55
D13 Third party products	0	0	10	4	14
D16 Statement of accounts	5	0	18	4	27
D20 Direct debit arrangements	5	0	2	0	7
D21 Chargebacks	1	0	1	0	2
D21.3 Recurring payment arrangements	0	0	0	0	0
D22 Closure of accounts	0	0	2	3	5
D26.5 Centrelink requirements	0	0	0	0	0
Provision of credit	4	2	134	28	168
Credit assessment, responsible lending and financial difficulty	3	0	120	28	151
KP4 We will be responsible lenders	1	0	5	0	6

Service Standards	Micro institution	Small institution	Medium institution	Large institution	Total
D6 Responsible lending practices	1	0	115	27	143
D7 Credit limit increase offers	0	0	0	0	0
D24 If you are in financial difficulties	1	0	0	1	2
Joint debtors, accounts & sub. cards	0	1	10	0	11
D9 Joint accounts	0	1	8	0	9
D10 Subsidiary cards	0	0	2	0	2
D11 Safeguards for co-borrowers	0	0	0	0	0
Other provision of credit obligations	1	1	4	0	6
D8 Reverse mortgage loans	0	0	0	0	0
D12 Safeguard for loan guarantors	0	0	2	0	2
D26 Debt collection and legal action	1	1	2	0	4
Other Code obligations (such as Training, Privacy, IDR)	17	19	50	293	379
Privacy and confidentiality	15	15	233	31	294
D23 Information privacy and security	15	15	233	31	294
Advertising	0	3	14	4	21
D1 Advertising	0	3	14	4	21
Communication	1	0	14	3	18
D15 Timely, clear and effective	1	0	12	2	15
D18 Electronically	0	0	2	1	3
D25 Working with your representative	0	0	0	0	0
Training	0	0	5	0	5
D14 Use of finance brokers	0	0	0	0	0
E2 Training our staff	0	0	5	0	5
Dispute Resolution	1	1	38	1	41
KP6 Deal fairly with any complaints	0	0	0	0	0
D27 Prompt, fair resolution of complaints	0	0	38	1	39
D28 Our complaints handling process	0	1	0	0	1
D29 External Dispute Resolution (EDR)	1	0	0	0	1
D30 Complaints about Code breaches	0	0	0	0	0
Promotion of the Code	0	0	0	0	0
B Commitment to comply with Code	0	0	0	0	0
KP10 Support and promote Code	0	0	0	0	0
E1 Publicising the Code	0	0	0	0	0
Grand Total	90	48	176	902	1,216

Appendix D: Significant self-reported Code breaches in 2016–17

KP7 'We will recognise our customers' rights as owners'	
Details	Customers were charged a penalty rate for Term Deposit changes within the grace/cooling-off period. This breach was reported to ASIC.
Cause	Core Banking system allowed operators discretion to redeem at penalty or at full rate. Incorrect selection was made by operators.
Exposure	9,688 accounts were affected from 1 August 2014 to 13 July 2017. A total amount of \$104,129.02 was paid to customers on 8 August 2017.
Outcome	The matter was reported to ASIC. Remedial work included refunds to customers and a change to the Core Banking System to prevent staff from choosing 'redeem at penalty' during the grace/cooling-off period.
K2 'Information about our products'	
Details	One significant breach of the Code relating to misleading conduct to members during the sale of a certain 'Reward' product. This breach was reported to ASIC. The 'Reward' product is an online savings account designed to encourage customer to deposit their salary into one of the everyday transaction accounts and make the institution their 'main' bank. The product offers customers additional or bonus interest on funds held in the product after customers deposit at least \$1,000 into a separate and linked everyday transaction account. Customers are offered additional interest on funds in the 'Reward' product up to a limit of \$100,000.
Cause	Based on feedback from customers, the cause of the 'Reward' product incidents related to two issues around a misunderstanding about the features of the product. These must be satisfied to receive the bonus interest payment. Issue 1: the requirement for \$1,000 or more to be deposited into one of the 'everyday' transaction accounts. Instead, customers have been depositing the \$1,000 in the 'Reward' product itself. Issue 2: the bonus interest is limited to the first \$100,000 invested into the product, meaning balances over this amount do not receive the bonus interest. Only two customers fell into this group.
Exposure	43 breaches were recorded (e.g. 43 customers were impacted) across the network over a period of ten months. The institution has since compensated all customers with lost interest where the \$1,000 requirement has been met but where the funds were erroneously allocated to the 'Reward' product rather than a transaction account, and members with 'Reward' balances over \$100,000. The total financial impact or compensations provided was \$16,214. It is important to point out that even where customers felt that they had been informed incorrectly about the 'Reward' product and had complained as a result, with one

	exception none of these customers subsequently moved their funds out of the institution, or to another financial product.
Outcome	To address this issue, the key improvements the institution made included: <ul style="list-style-type: none"> - product collateral was improved to better explain key requirements of the 'Reward' product - communications were provided to sales teams iterating the 'Reward' products features and conditions - sales leadership provided additional training with retail branch staff - required sales staff to complete an internal exam on product features via internal training systems to ensure currency of knowledge and competence - point of sale material now distils the 'Reward' product's features and simplifies the messaging to members; and - post-sale material also now confirms the 'Reward' account's operation and key features.

D17 'Notifying changes to your account'

Details	Customers were not provided with confirmation of transactions for financial products as required by s1017F Corporations Act 2001. The incident is limited to a failure to provide confirmation of the acquiring or disposing of a direct debit facility.
Cause	The confirmation of transactions for direct debit facilities, which are incorporated into the account statements, did not include notification of the acquisition or disposal of direct debit facilities. The investigation identified that an error in the coding used to generate the information to be reported, which resulted in all direct debit supplier codes except for one particular code being excluded rather than included in the report.
Exposure	85,109 customers did not receive confirmation of the acquisition or disposal during the period of April 2013 to September 2016.
Outcome	The error in the coding used to generate the report for meeting the disclosure obligations of s1017F has been corrected. Therefore, all accounts statements for the period ending 31 October 2016 and onwards will include the information required to confirm the acquisition and disposal of direct debit facilities. All 85,109 clients who did not receive confirmation of the acquisition or disposal of a direct debit facility have received this notification with their account statements for the period ending 31 December 2016.

Key Promise 4 'We will be responsible lenders'

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

D17 'Notifying changes to your account'

Details	Loan funds were transferred to an incorrect account, and the funds used by the other member.
Cause	Error in processing.
Exposure	\$2,000
Outcome	Arrangement for member to repay overdrawn account – original member received the funds.

Appendix E: Comparative table of self-reported complaints

Table 15: Number of self-reported IDR complaints

	Category	2012-13		2013-14		2014-15		2015-16		2016-17	
Service/Products involved in complaints	Credit	1,345	9%	1,325	11%	1,608	9%	1,665	12%	2,987	16%
	Deposit Taking	2,166	15%	1,829	15%	1,930	12%	2,655	19%	7,444	40%
	General Insurance	132	1%	180	1%	263	2%	175	1%	349	2%
	Investments	29	<1%	68	<1%	230	1%	76	1%	1,950	10%
	Life Insurance	13	<1%	5	<1%	0	0%	3	<1%	49	0%
	Payment Systems	6,334	44%	4,075	33%	3,746	22%	3,789	27%	3,508	19%
	Traditional Trustee Services	0	0%	4	<1%	6	<1%	11	<1%	1,169	6%
	Other ²⁰	4,374	30%	4,923	40%	8,926	53%	5,726	41%	1,206	6%
Issues involved in customer complaint	Advice	84	1%	100	1%	413	2%	705	5%	857	5%
	Charges	1779	12%	2,026	16%	4,792	29%	2,829	20%	2,131	11%
	Disclosure	211	1%	211	2%	279	2%	334	2%	1,810	10%
	Financial Difficulty/Responsible Lending	93	1%	157	1%	174	1%	117	1%	546	3%
	Decision by institution	239	2%	383	3%	565	3%	1,005	7%	3,887	21%
	Instructions	517	4%	903	7%	624	4%	1,093	8%	1,156	6%
	Privacy	140	1%	121	1%	103	1%	118	1%	223	1%
	Service	4,752	33%	4,822	39%	3,083	18%	4,318	31%	4,393	24%
	Transactions (incl. ATM issues)	3,859	27%	2,291	18%	3,104	19%	2,201	16%	2,180	12%
	Other	2,719	19%	1,395	11%	3,572	22%	1,380	10%	1,479	8%
Outcome of customer complaint	In favour of customer	3,935	27%	4,371	35%	6,022	36%	4,968	35%	4,806	26%
	In favour of institution	1,181	8%	1,335	11%	822	5%	1,013	7%	2,493	13%
	Customer taken legal action	1	<1%	1	<1%	8	<1%	3	<1%	4	0%
	Mutual agreement	6,812	47%	5,941	48%	3,228	19%	3,117	22%	6,213	33%
	Referred to External Dispute Resolution	206	1%	92	1%	177	1%	258	2%	247	1%
	Withdrawn	322	2%	199	2%	119	1%	123	1%	376	2%
	Apology, explanation, acknowledgement, feedback	n/a	n/a	n/a	n/a	5,675	34%	3,704	26%	3,828	21%
	Outstanding	1,647	11%	45	<1%	50	<1%	80	1%	226	1%
	Other	289	2%	425	3%	608	4%	834	6%	469	3%
Timeframe	Resolved within 21 days	12,637	88%	10,768	87%	15,606	93%	13,078	93%	16,725	90%
	Resolved within 45 days	932	6%	920	7%	797	5%	571	4%	1,149	6%

²⁰ 'Other' represents the number of complaints that were not further specified by institutions.

	Category	2012-13		2013-14		2014-15		2015-16		2016-17	
	Resolved beyond 45 days	135	1%	317	3%	256	2%	185	1%	501	3%
	Unresolved as at 30 th June	337	2%	45	0%	50	0%	80	1%	155	1%
	Other	352	2%	359	3%	0	0%	186	1%	132	1%
Number of self-reported IDR complaints which include Code breaches											
		309	2%	370	3%	233	1%	256	2%	242	1%
Total number of self-reported IDR complaints											
		14,393		12,409		16,709		14,100		18,662	
Number of institutions that self-reported IDR complaints											
		82	90%	79	89%	70	88%	65	89%	59	88%

Appendix F: Additional tables – complaints data by institution size

Table 16: Number of self-reported IDR complaints by institution size in 2016-17

	Category	Micro institution	Small institution	Medium institution	Large institution	Total
Service/Products involved in complaints	Credit	33	56	206	2,692	2,987
	Deposit Taking	85	125	500	6,734	7,444
	General Insurance	1	0	41	307	349
	Investments	7	9	62	1,872	1,950
	Life Insurance	0	0	7	42	49
	Payment Systems	44	25	273	3,166	3,508
	Traditional Trustee Services	143	109	131	786	1,169
	Other ²¹	10	1	207	988	1,206
Issues involved in customer complaint	Advice	2	1	14	840	857
	Charges	11	39	102	1,979	2,131
	Disclosure	27	7	36	1,740	1,810
	Financial Difficulty	12	4	10	520	546
	Decision by institution	13	9	249	3,616	3,887
	Instructions	25	34	121	976	1,156
	Privacy	17	7	35	164	223
	Service	28	159	511	3,695	4,393
	Transactions (incl. ATM issues)	173	23	203	1,781	2,180
	Other	15	42	146	1,276	1,479
Outcome of customer complaint	In favour of customer	206	173	276	4,151	4,806
	In favour of institution	20	62	130	2,281	2,493
	Customer taken legal action	0	1	0	3	4
	Mutual agreement	63	43	429	5,678	6,213
	Referred to External Dispute Resolution	3	6	13	225	247
	Withdrawn	10	1	27	338	376
	Apology, explanation,	16	38	510	3,264	3,828

²¹ 'Other' represents the number of complaints that were not further specified by institutions.

	Category	Micro institution	Small institution	Medium institution	Large institution	Total
	acknowledgement, feedback					
	Outstanding	1	1	6	218	226
	Other	4	0	36	429	469
	Resolved within 21 days	254	285	1,354	14,832	16,725
	Resolved within 45 days	36	30	33	1,050	1,149
	Resolved beyond 45 days	10	8	25	458	501
	Unresolved as at 30 th June	1	1	7	146	155
	Other	22	1	8	101	132
Grand total		323	325	1,427	16,587	18,662

Appendix G: Additional tables – breach & complaints data

Table 17: Total number and mean of self-reported Code breaches by size of institution

	2012–13		2013–14		2014–15		2015–16		2016–17	
	Total	Mean ²²	Total	Mean	Total	Mean	Total	Mean	Total	Mean
Reported by all institutions	917	10.1	800	8.9	646	8.1	818	11.2	1,216	18.1
Reported by										
- large institutions	287	13.0	269	12.2	447	21.3	456	28.5	902	53.1
- medium institutions							211	14.1	176	12.6
- small institutions	520	18.6	455	16.3	119	4.8	49	3.1	48	4.4
- micro institutions	110	2.7	76	1.9	80	2.4	102	3.9	90	3.6

Table 18: Number of institutions self-reporting Code breaches

Number of self-reported Code breaches	Number of institutions				
	2012–13	2013–14	2014–15	2015–16	2016–17
Nil breaches	35	39	31	24	16
Between 1 to 10 breaches	39	32	33	27	29
Between 11 to 20 breaches	7	10	5	8	6
Between 21 to 50 breaches	7	6	9	9	11
Between 51 to 100 breaches	2	1	2	5	3
Over 100 breaches	1	1	0	0	2

Table 19: Total number and mean of self-reported IDR complaints by size of institution

	2012–13		2013–14		2014–15		2015–16		2016–17	
	Total	Mean ²³	Total	Mean	Total	Mean	Total	Mean	Total	Mean
Reported by all institutions	14,393	158.2	12,409	139.4	16,709	208.9	14,100	193.2	18,662	278.5
Reported by										
- large institutions	11,292	513.3	9,732	442.4	14,107	671.8	11,215	700.9	16,587	975.7
- medium institutions							1,815	121.0	1,427	101.9
- small institutions	2,552	91.1	2,191	78.2	1,970	78.8	747	46.7	325	29.5
- micro institutions	549	13.4	486	12.5	632	18.6	324	12.5	323	12.9

Table 20: Number of institutions self-reporting IDR complaints

Number of self-reported IDR complaints	Number of institutions				
	2012–13	2013–14	2014–15	2015–16	2016–17
Nil complaints	9	10	10	8	8
Between 1 to 10 complaints	23	29	18	19	20
Between 11 to 20 complaints	13	14	8	9	4
Between 21 to 50 complaints	18	10	17	11	11
Between 51 to 100 complaints	8	6	6	9	7
Between 101 to 1,000 complaints	17	18	18	13	14
Over 1,000 complaints	3	2	3	4	3

²² Average based on total number of Code breaches divided by number of institutions.

²³ Average based on total number of customer complaints divided by number of institutions.

Appendix H: Definitions

Categorisation of Code Subscribers

Since 2015-16, the size of institutions are categorised based on \$ amount in assets (prior to that size of institutions were measured by number of staff):

Size of institution	prior 2015-16 measured by staff numbers	since 2015-16 measured by \$ amount in assets
Large	over 100 full time equivalent staff	over \$1b in assets
Medium	31-100 full time equivalent staff	\$500m to \$1b in assets
Small	up to 30 full time equivalent staff	\$200m to \$500m in assets
Micro	included in above	up to \$200m in assets

Financial Ombudsman Service (FOS) Australia

The Financial Ombudsman Service (FOS) Australia (Compliance Manager²⁴) provides Code monitoring and administration services to the Committee and COBA by agreement. FOS has appointed a dedicated team of staff (Code Team) within its office to undertake that task.

²⁴ As per Customer Owned Banking Code Compliance Committee Charter section 4.4.