CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

ANNUAL REPORT 2014–2015

Customer Owned Banking Code of Practice

December 2015

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 2014 to 30 June 2015.

Data has been collated from monitoring the activities of the 80 institutions that subscribed to the Code in 2014–15, and consists of the outcomes of an Own Motion Inquiry, the 2015 Annual Compliance Statement and investigations into alleged Code breaches.

This report also reviews the Customer Owned Banking Code Compliance Committee's monitoring activities from 1 July 2014 to 30 June 2015, and shares its 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.

FOREWORD

On 1 July 2014, the customer owned banking industry formally adopted the revised Customer Owned Banking Code of Practice. This Code establishes a good practice benchmark for industry and is a clear statement of the commitment customer owned banking institutions have made to their customers.

Eighty credit unions, mutual banks and mutual building societies voluntarily subscribed to the Code in 2014–15, with all taking part in the Committee's Annual Compliance Statement (ACS) program. Our findings confirm that these institutions are strongly committed to achieving the Code's standards.

Participants in our ACS program collectively reported 646 breaches of the Code, 154 (19%) less than the previous reporting period. Most breaches related to privacy and security obligations, with recent revisions to the Privacy Act appearing to prompt more proactive reporting in this area. Code Subscribers also reported one less significant breach compared to 2013–14. The nature and extent of significant breaches is an important indicator of Code compliance as, by definition, these breaches have the most impact on customers. We are pleased to report that all breaches have been remedied, or that remedial action is underway.

In light of these results, we expected a corresponding reduction in customer complaints, yet Code Subscribers reported 16,709 complaints, up 35% on 2013–14. Our verification program, which tests and validates Code Subscribers' compliance programs, suggests there may be some inconsistencies and inaccuracies in complaints and breach reporting. Given these findings – and the fact that more than a third of participants reported no Code breaches – we will redouble our efforts to work with the Customer Owned Banking Association (COBA) and Code Subscribers to achieve consistent reporting that reflects a true position of industry performance.

While we acknowledge Code Subscribers' genuine and ongoing commitment to help their customers who are experiencing financial difficulty, service standards in this area remained a significant source of consumer complaint in 2014–15. We encourage Code Subscribers to consider the results of our Own Motion Inquiry into compliance with financial difficulty obligations – detailed on page 28 of this report – which offers valuable insights into good industry practice. We have also published guidelines on our website to help consumers understand their rights and responsibilities under the Code should they find themselves in financial hardship.

Throughout 2014–15 we consulted with a range of stakeholders to influence positive changes in industry behaviour and share our experience of Code compliance. Members of our Committee and Secretariat attended more than 25 meetings involving COBA, the Australian Securities and Investments Commission, the Credit and Investments Ombudsman, Code Subscribers and consumer and small business representatives.

Our Secretariat also provided Code training to more than 200 financial counsellors through partnerships with the Financial and Consumer Rights Council, and the Telecommunication

Industry Ombudsman and Energy and Water Ombudsman schemes in Victoria, NSW and South Australia.

Over the coming year, the Committee will make our Code monitoring and investigation services even more accessible as we finalise a plain English review of our website content, develop a user-friendly online feedback form for consumers and their representatives, and strengthen our Code awareness program for consumer advocates and community lawyers.

We have achieved significant outcomes this year thanks to the support of our dedicated Secretariat. Under the leadership of General Manager Dr June Smith, Secretariat staff continued to improve the efficiency of our operations through an enhanced Code database and a secure online portal, which has streamlined the Committee's exchange of information with Code Subscribers.

On 1 July 2015, June was appointed to the position of Lead Ombudsman (Investments and Advice) at the Financial Ombudsman Service (FOS) Australia. We would like to thank her for her outstanding work with the Committee over the past four years and wish her every success in her new positon. We also thank Anita Schut for her continuing dedication to Code Subscribers as industry representative and Professor Gail Pearson for her exceptional work as consumer representative over the past year. We extend a warm welcome to Carolyn Bond as the newly appointed consumer representative, and to Sally Davis as the new General Manager, Code Compliance & Monitoring.

Thank you to everyone who has engaged with us over the past year. We look forward to working with you in 2015–16 to continue to meet and exceed the Code's standards of good industry practice.

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

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

2014–15: YEAR AT A GLANCE

80

customer owned banking institutions subscribed to the Code

5

significant Code breaches were self-reported by 5 Code Subscribers (page 16)

61%

of institutions self-reported Code breaches

▲ 5%

from the previous year (page 13)

646

Code breaches were self-reported by institutions

26%

of self-reported breaches related to training obligations (page 13)

20%

of self-reported breaches related to privacy obligations (page 13)

88%

of institutions self-reported 16,709 complaints handled by their internal dispute resolution process

▲ 35%

from the previous year (page 17)

93%

of complaints were resolved within 21 days or less

29%

of complaints related to charges (page 21)

18%

of complaints related to services (page 21)

Analysed 80 Annual Compliance Statements
See page 11 ➔

Reviewed two alleged Code breaches
See page 26 ➔

Published guidance regarding Code compliance with financial difficulty obligations
See page 28 ➔

Verified compliance with 14 selected institutions
See page 24 ➔

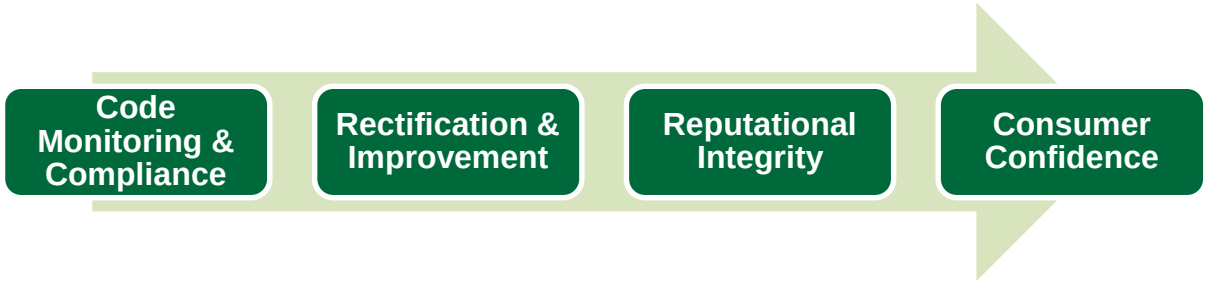
Developed a Code monitoring framework and risk assessment model
See page 11 ➔

Took part in 13 Code training sessions and presentations
See page 29 ➔

Hosted 1 consumer advocate meeting
See page 29 ➔

ABOUT THE CODE

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



The Code outlines the commitment to comply with its obligations and its relation to other laws and regulations. This includes:

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

By subscribing to this Code, customer owned banking institutions have voluntarily committed to abide by good industry practice, promote informed decision-making about their services, and act fairly and reasonably in delivering those services.

They have also committed to deliver on their pledge to always put customers first by subscribing to the Code's 10 key promises. These promises apply to all customer owned banking services delivered to individuals and small business across Australia by Code Subscribers.

The Code's 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.

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. Code Subscribers as at 30 September 2015 are listed in **APPENDIX A.**

COBA and its members believe that the Code establishes a good practice benchmark for industry and is a clear statement of the commitment institutions make to their customers. The Code is a market leading, plain English document. It provides customers with the confidence to be treated fairly and responsibly by the customer owned banking industry.

ABOUT THE CODE COMPLIANCE COMMITTEE

The Code Compliance 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 COBA. It supports customer owned banking institutions to achieve service standards Australians can trust.

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. It 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 five key 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
5. **Accessibility** to its Code monitoring and investigation services

Committee functions

The Committee's Code monitoring and compliance activities are structured along three core streams:

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

In 2014–15, the Committee met formally six times; one of these meetings was held via teleconference.

Secretariat

The Financial Ombudsman Service (FOS) Australia Code team (the Secretariat) continued to provide Code monitoring and administration services to the Committee and COBA by agreement.

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 2016

Sue-Anne has extensive experience in the not-for-profit sector. She is Chair of the Australian Council for International Development's Code of Conduct, Vice-President Humanitarian Quality Assurance Initiative (Geneva), Executive Chairman of Creating Australia and director of several other organisations. For the past 12 years, she 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.

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

Appointed: 1 January 2014
Term expires: 31 December 2016

Anita is the Compliance Manager at Maritime Mining and Power Credit Union. She has more than 12 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.

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 for 15 years (including the Consumer Action Law Centre).

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, Energy and Water Ombudsman Victoria Board, the Banking and Financial Services Ombudsman Board and the Commonwealth Consumer Affairs Advisory Committee.

Professor Gail Pearson
BA (Hons), LLB, PhD
Consumer Representative
Appointed: 26 February 2014[2]
Term expired: 26 February 2015

Gail was a founding member of the Committee and a leading academic and author in financial services and commercial and consumer law, and co-founder of the Australasian Consumer Law Roundtable. She is President of the International Association of Consumer Law (outgoing) and a member of the International Law Association Committee, which drafted the Sofia Principles for international protection of consumers.

[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] Appointed under the revised Code (section 5.5). Previous term under 2010 Mutual Banking Code of Practice: 1 October 2009 to 30 September 2011, including re-appointment.

SECRETARIAT STAFF

Dr June Smith
General Manager
Code Compliance & Monitoring
BA (Hons) LLB, PhD
Appointed: July 2011 – 30 June 2015

June is a specialist in integrity, governance and self-regulatory frameworks. She is a lawyer with a PhD in applied ethics and organisational decision-making within financial services organisations. During the reporting year June held a number of external appointments in addition to her role as General Manager, including Chair of the Financial Planning Association of Australia's Conduct Review Commission, Chair of the Code Compliance Monitoring Committee - Australian Travel Agents Scheme, Member of Racing Victoria's Racing Appeals and Disciplinary Board, Advisory Member, Member Compliance Committee – Financial Consumer Rights Council of Victoria and Victoria University Alumni Ambassador.

On 1 July 2015 June commenced in the role as Lead Ombudsman (Investments and Advice) with the Financial Ombudsman Service Australia.

Daniela Kirchlinde
Compliance Manager
BComm, Grad Dip (Finance and Investment)
Appointed: October 2009 – current

Daniela has a background in dispute resolution and broad insurance industry experience in Australia, England and Germany. In addition to her Compliance Management role, she manages compliance for the Insurance Brokers Code of Practice.

Sally Davis
General Manager
Code Compliance & Monitoring
BComm, LLB, Grad Dip (Arts)
Appointed: September 2015 – current

Sally has been appointed as General Manager of Code Compliance and Monitoring at the Financial Ombudsman Service (FOS) Australia effective 1 September 2015. The appointment has been made on the recommendation of a selection committee comprising Mr Christopher Doogan, Independent Chair of the Code Compliance Monitoring Committee (banks), Dr Sue-Anne Wallace, Independent Chair of the Code Compliance Committee (customer owned banking institutions), and Mr Shane Tregillis, Chief Ombudsman, FOS.

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

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 framework, while providing the Committee with robust data on Code compliance among subscribers.

Annual Compliance Statement program

The Annual Compliance Statement (ACS) is a self-assessment tool that helps Code Subscribers review their compliance with Code obligations every year, as required under section E21 of the Code.

The 2014–15 ACS was developed with COBA and other stakeholders to achieve a consistent compliance monitoring approach. It 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.

See pages 33 to 44 for an analysis of the aggregated data drawn from the 2014–15 ACS program.

ANNUAL COMPLIANCE STATEMENT OUTCOMES

The aggregated breach data in this section reflects the outcomes of Code Subscribers' internal Code monitoring activities during 2014–15, in accordance with their Code monitoring obligations. This data is collected from Code Subscribers via the Annual Compliance Statement (ACS) program.

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. This differs to a **significant breach** of Code obligations, which 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 via its ACS program since 2012–13. The nature and extent of the identified significant breaches is an important indicator of Code compliance as, by definition, these breaches have the most impact on customers. Often these breaches, together with remedial actions taken by Code Subscribers, would have been 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.

In 2014–15, 61% of the participating Code Subscribers reported breaches of the Code in comparison to 56% for the previous reporting period (see **APPENDIX F**). The Committee will continue to assist Code Subscribers with their compliance processes and encourage positive breach reporting to ensure that it reflects an accurate reflection of their performance.

Self-reported Code breaches

Key findings

Note the percentage in square brackets represent comparison figures for the 2013–14 period.

- 646 Code breaches were self-reported by Code Subscribers, a decrease of 154 (19%) on the 800 breaches reported last year.
- 61% *[56%]* of customer owned banking institutions self-reported Code breach activity.
- Eight Code Subscribers collectively accounted for 348 Code breaches[3], 54% of the total breaches reported in 2014–15. One Code Subscriber reported 70 Code breaches, mainly relating to privacy issues regarding obligations under Sections C8 and D23.
- 26% of the reported breaches related to training (Section C5).
- 20% of the reported breaches related to privacy and security obligations (Section D23), with another 24% of the reported breaches related to complying with legal and industry obligations (Section C8), also including privacy obligations.
- The increase in reported breaches in those Sections relating to privacy obligations appears to be primarily attributed to the revision of the Privacy Act in March 2014. These breaches provide a timely reminder to staff of their obligations under the Act and the new rules and appear to have prompted more proactive reporting of breaches. The breaches were addressed following each occurrence by raising staff awareness and refresher training being provided to relevant staff on privacy obligations. Guidelines and frequently asked questions were also provided to assist them to understand and comply with privacy requirements.
- Most breaches reported were identified through quality assurance programs.
- 36% *[46%]* breaches were identified as a result of customer complaint investigations.

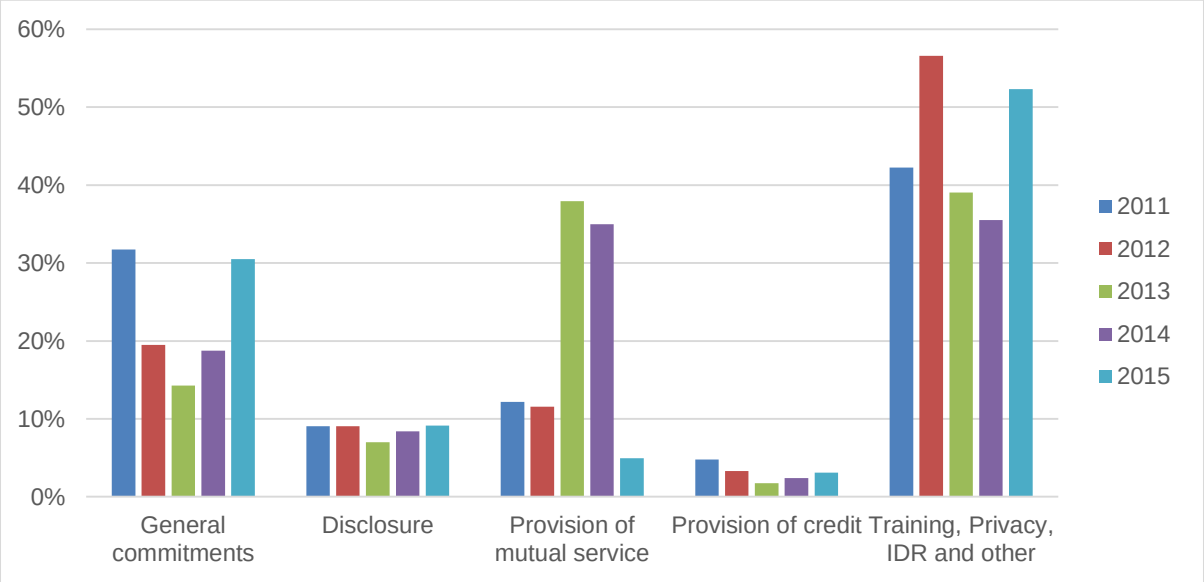
[3] These Code Subscribers reported in excess of 30 Code breaches.

Self-reported Code breaches by category

Chart 1 below identifies the total number of self-reported Code breaches across five broad categories of Code obligations. These breaches are compared to the number of breaches reported in the same categories for the previous four reporting years.

The chart shows that in 2014–15, 82% of the total number of Code breaches reported related to 'Training, Privacy, Internal Dispute Resolution (IDR) and Other' (338 breaches or 52%) and 'General Commitments' (197 breaches or 30%).

Chart 1: Self-reported breaches by Code category 2011–15



Self-reported Code breaches by section

Chart 2 on page 15 examines major areas of non-compliance by Code Section in 2014–15, comparing these results with the previous four reporting years. Key findings are as follows:

- Key Commitments (Key promises 1, 2, 7, 8 and 9) – 156 breaches (24%) compared to 129 breaches (16%) in 2013–14. Most of these breaches refer to **Key Promise 8** ***'We will comply with our legal and industry obligations'*** – 110 breaches (17%) compared to 89 breaches (69%) in 2013–14, in particular regarding privacy and security issues. The increase in reported breaches compared to the previous period can be attributed to revision of the Privacy Act in March 2014, which provided a timely reminder to staff of their obligations under the Act and the new rules, prompting more proactive reporting of breaches in this area.

- **Section D23** ***'Privacy & Security'*** – 129 breaches (20%) compared to 105 breaches (13%) in 2013–14.

- Training, mainly involving breaches of **Key Promise 5** ***'We will deliver high customer service and standards'*** – 165 breaches (26%) compared to 132 breaches (17%) in 2013–14.

- Information about products and services including 33 breaches (5%) of **Key Promise 3** ***'We will give you clear information about our products and services'*** and 31 breaches (5%) of **Section D2** ***'Information about our products'***. This compares to 29 breaches (4%) and 20 breaches (3%) respectively in 2013–14.

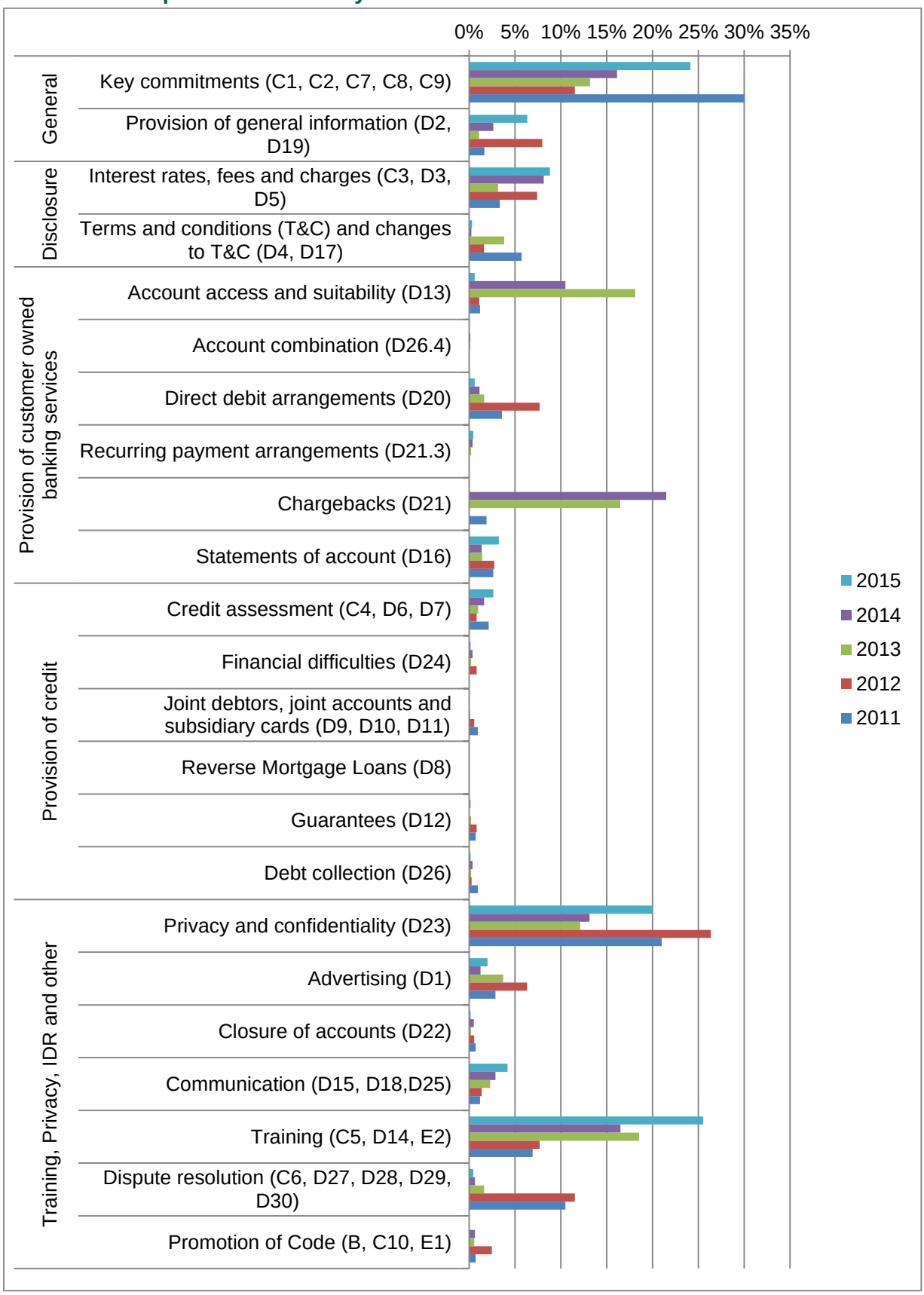
- **Communication** (Sections 15, 18 and 25), mainly referring to ***'Timely, clear and effective communication'*** – 27 breaches (5%) compared to 23 breaches (3%) in 2013–14.

Of the institutions that reported more than 30 breaches, eight institutions reported 348 breaches (57%) in 2014–15. This compares to 217 breaches (27%) reported by two institutions in 2013–14.

For a full comparative analysis table of all self-reported Code breach data from 2010–11 to 2014–15, see **APPENDIX B** and **APPENDIX F.**

For de-identified examples of breaches self-reported by Code Subscribers, including breach details and remedial actions, see **APPENDIX C**.

Chart 2: Self-reported breaches by Code section 2011–15



Self-reported significant breaches

Five significant breaches were reported in 2014–15 by five Code Subscribers, compared to six significant breaches reported by five Code Subscribers in 2013–14. **APPENDIX D** contains information on these breaches, including the status of remedial actions.

These significant breaches are represented by Code category in **Table 1** below and cover Code obligations regarding:

- Key Commitment 8 ***'We will comply with our legal and industry obligations'***
- Section D2 ***'Information about our products'***
- Section D16 ***'Account statements and balances'***, and
- Section D23 ***'Information privacy and security'***.

It is pleasing to note that remedial actions to address all Code breaches have either been completed or are underway.

Table 1: Self-reported significant breaches by Code category 2013–2015

Group	Code category	2012/2013	2013/2014	2014/2015
General	Key commitments (C1, C2, C7, C8, C9)	3	2	1
	Provision of general information (D2, D19)	1	0	1
	TOTAL GENERAL	**4**	**2**	**2**
Disclosure	Interest rates, fees and charges (C3, D3, D5)	2	0	0
	Terms and conditions (T&C) and changes to T&C (D4, D17)	1	1	0
	TOTAL DISCLOSURE	**3**	**1**	**0**
Provision of customer owned banking services	Statements of account (D16)	1	0	1
	TOTAL PROVISION OF CUSTOMER OWNED BANKING SERVICES	**1**	**0**	**1**
Provision of credit	Credit assessment (C4, D6, D7)	1	0	0
	TOTAL PROVISION OF CREDIT	**1**	**0**	**0**
Training, Privacy, IDR and other	Privacy and security (D23)	1	1	2
	Advertising (D1)	1	1	0
	Communication (D15, D18, D25)	0	1	0
	Promotion of Code (B, C10, E1)	5	0	0
	TOTAL TRAINING, PRIVACY, IDR and OTHER	**7**	**3**	**2**
TOTAL significant self-reported breaches		16	6	5
Number of institutions that self-reported significant breaches		*9*	*5*	*5*

Code Subscribers' compliance initiatives

Individual Code Subscribers introduced several initiatives to improve Code monitoring programs and reporting processes in 2014–15.These have strengthened compliance risk assessment processes and further embedded compliance requirements within their businesses and across the industry. Initiatives included:

- reviewing and enhancing breach and complaint registers
- providing periodic Code refresher training for staff, as well as training in specific areas such as complaint and dispute handling
- monitoring and supervising staff to improve their compliance performance, and providing tools such as compliance checklists
- conducting spot checks and 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, and
- reviewing documents, product terms and conditions, and website information to ensure they comply with Code requirements.

Internal Dispute Resolution complaints

Key findings

Note the percentage in square brackets represent comparison figures for the 2013–14 period.

- 88% *[89%]* of Code Subscribers self-reported a total of 16,709 *[12,409]* complaints handled by their internal dispute resolution process.
- 12% *[11%]* of Code Subscribers reported no complaints.
- The major product/service areas for customer complaints in 2014–15 concerned payment systems (22%) and deposit taking (12%). For 53% *[40%]* of complaints, Code Subscribers did not provide further details regarding the product/service involved.
- 29% *[16%]* of complaints related to charges, 18% *[39%]* of complaints related to service issues and 19% *[18%]* of complaints related to transaction issues, including ATM transactions. 8% *[11%]* of complaints did not identify issues involved.
- 36% *[35%]* of complaints were resolved in favour of the customer and 19% *[48%]* of complaints were resolved by mutual agreement. 34% of complaints were resolved as an apology, explanation and/or acknowledgement of feedback which was a new category introduced in this year's ACS. Together, these three categories comprise 89% of the complaints' outcomes.
- 29% *[31%]* of complaints were resolved within 21 days, and 64% were either resolved on the spot (22%) or within five days (42%).

- The category ‘resolved on the spot’ was new in this year’s ACS. 91% of Code Subscribers advised that they report complaints which are resolved on the spot.
- 1% *[3%]* of complaints led to the identification of a breach of the Code.

The 2014–15 ACS requested the following aggregated complaints handling data recorded by Code Subscribers as part of their internal dispute resolution (IDR) systems:

- product/service area
- issues involved
- resolution outcomes, and
- timeframes to resolve disputes.

The Committee considered this information when it assessed Code Subscribers’ compliance with the following Code obligations:

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

Aggregate results collated from this data are outlined in **Chart 3** to **Chart 6** on pages 20 to 23.

For a full comparative analysis table of all self-reported complaints data from 2011–2015, see **APPENDIX E** and **APPENDIX F**.

FOS reported that it accepted 297 disputes against customer owned banking institutions in 2014–15 in its role as external dispute resolution provider.[4]

Issues attracting customer complaints

Effectively handling customer complaints in a professional and timely manner – including analysing their root causes – is important to maintaining the traditional leadership role of the industry in providing customer owned banking services.

While about half the Code Subscribers provided valuable comments and information in addition to the number of complaints, the high number of complaints reported without accompanying details of the product/service involved (53%) is a concern to the Committee. Institutions are encouraged to keep detailed records of complaints so that they can identify issues, develop processes to address these issues, and train staff in these processes.

The Committee is more concerned about the low number of complaints linked to a Code breach (1%) and encourages institutions to consider the critical connection between accurate complaints records and the ability to identify breaches of the Code.

[4] FOS Annual Review 2014–15, page 56

Based on institutions' additional comments, the following areas attracted a significant number of complaints:

Deposit taking:

- customer dissatisfaction with fees charged
- service issue whereby a staff member did not fully satisfy the customers' expectations, and
- term deposit roll overs.

Payment systems:

- duplicate transactions and chargebacks
- difficulties when using internet or phone banking
- ATM claims
- electronic banking down
- ATMs down, system errors, BPAY offline, and
- debit card issues.

Charges issues:

- individual fees
- ATM withdrawal fees, and
- new fee structures.

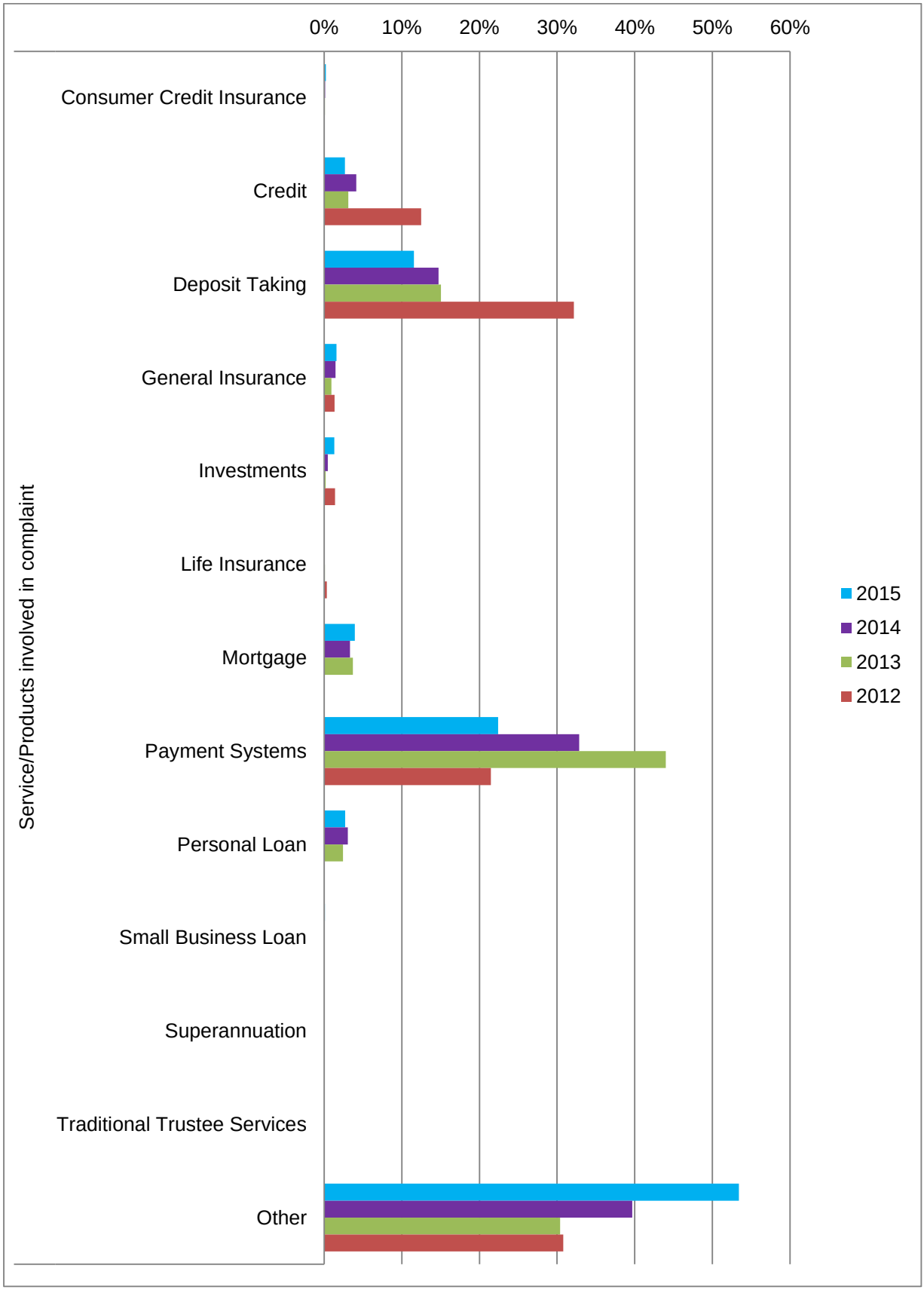
Services issues:

- implementation of new phone systems where the customers didn't like the options to choose from and on some occasions the length of time to answer the call
- service items related to branch renovations and relocations
- third-party products, e.g. internet banking password issues or issues with mobile applications
- service-related fees, and
- delays in processing loan applications.

Dispute resolution times

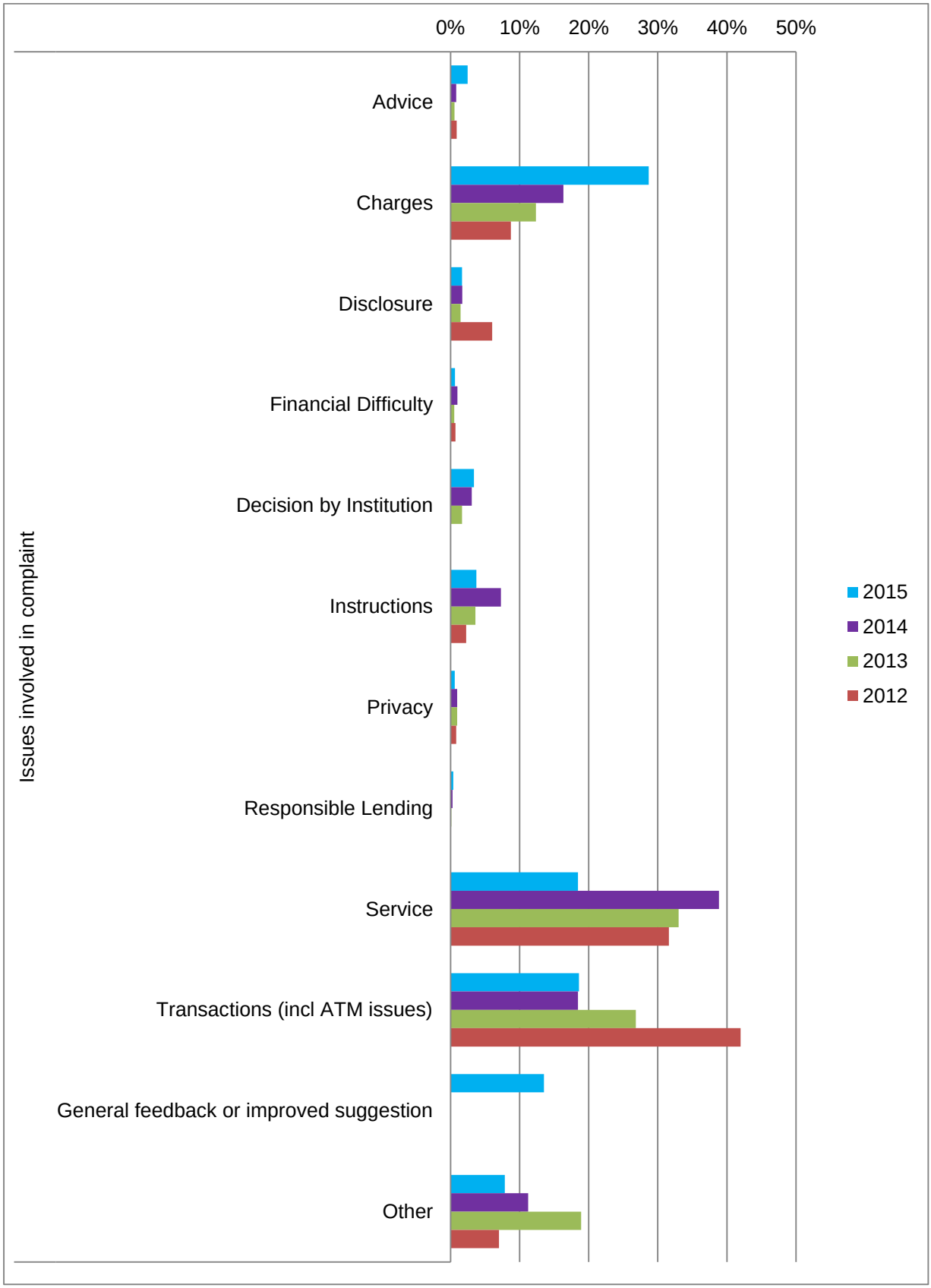
Code Subscribers resolved most customer complaints within 45 days, while 2% of complaints took more than 45 days to resolve (compared to 6% in 2013–14). Code Subscribers reported that most of these complaints took longer to resolve because they could not be settled internally and were subsequently lodged with an External Dispute Resolution scheme. They also attributed longer resolution times to the complexity of the complaint and to customers failing to provide required information in a timely manner. Two Code Subscribers reported that complaints were not closed correctly in their logging system at the time they were resolved with customers, resulting in longer resolution times being recorded.

Chart 3: Percentage of complaints by service/product involved 2012–15[5]



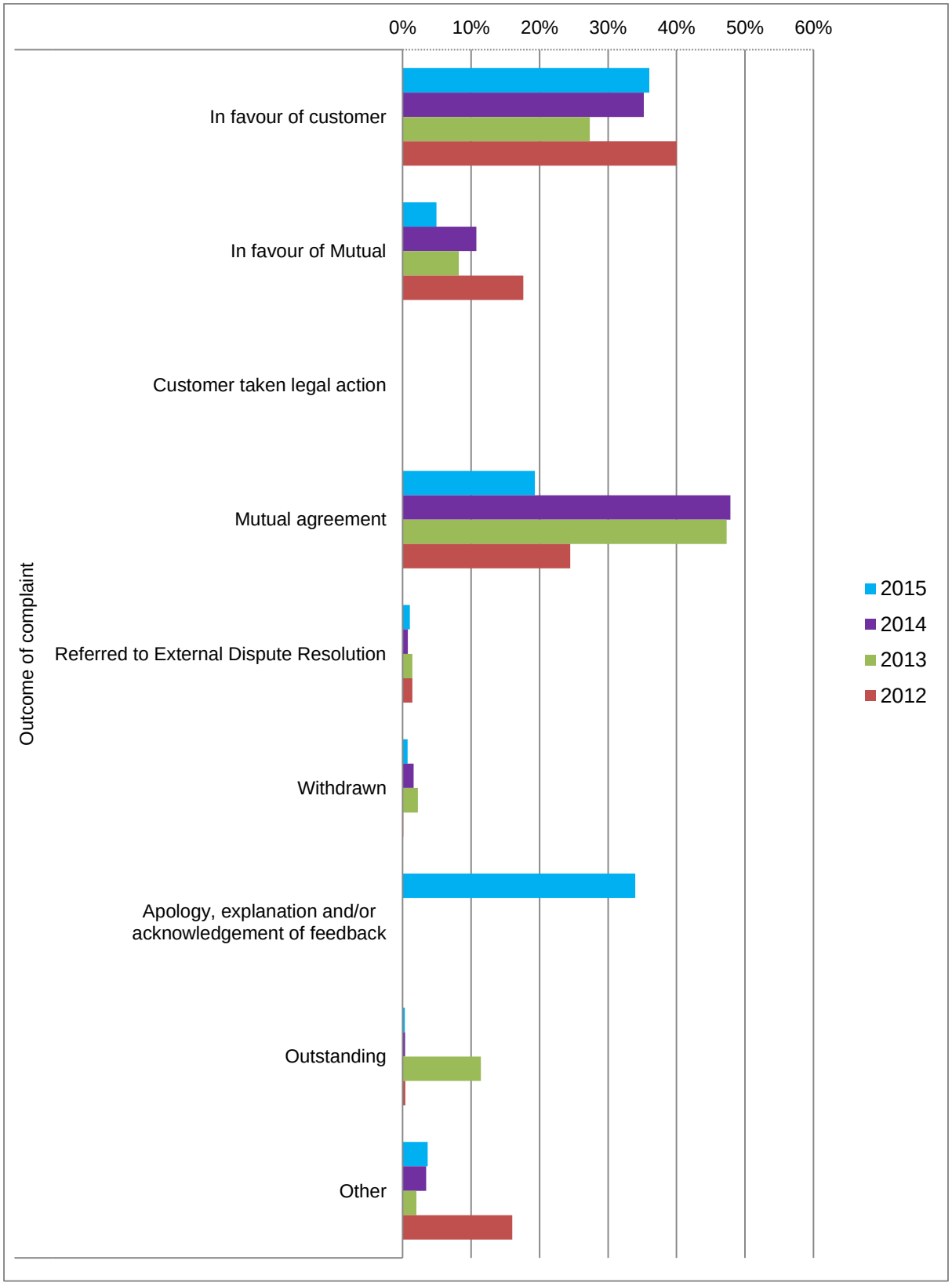
[5] 'Other' represents the number of complaints that were noted by the institution in the total number of complaints, but not further identified regarding the service/product involved.

Chart 4: Percentage of complaints by issues involved 2012–15[6]



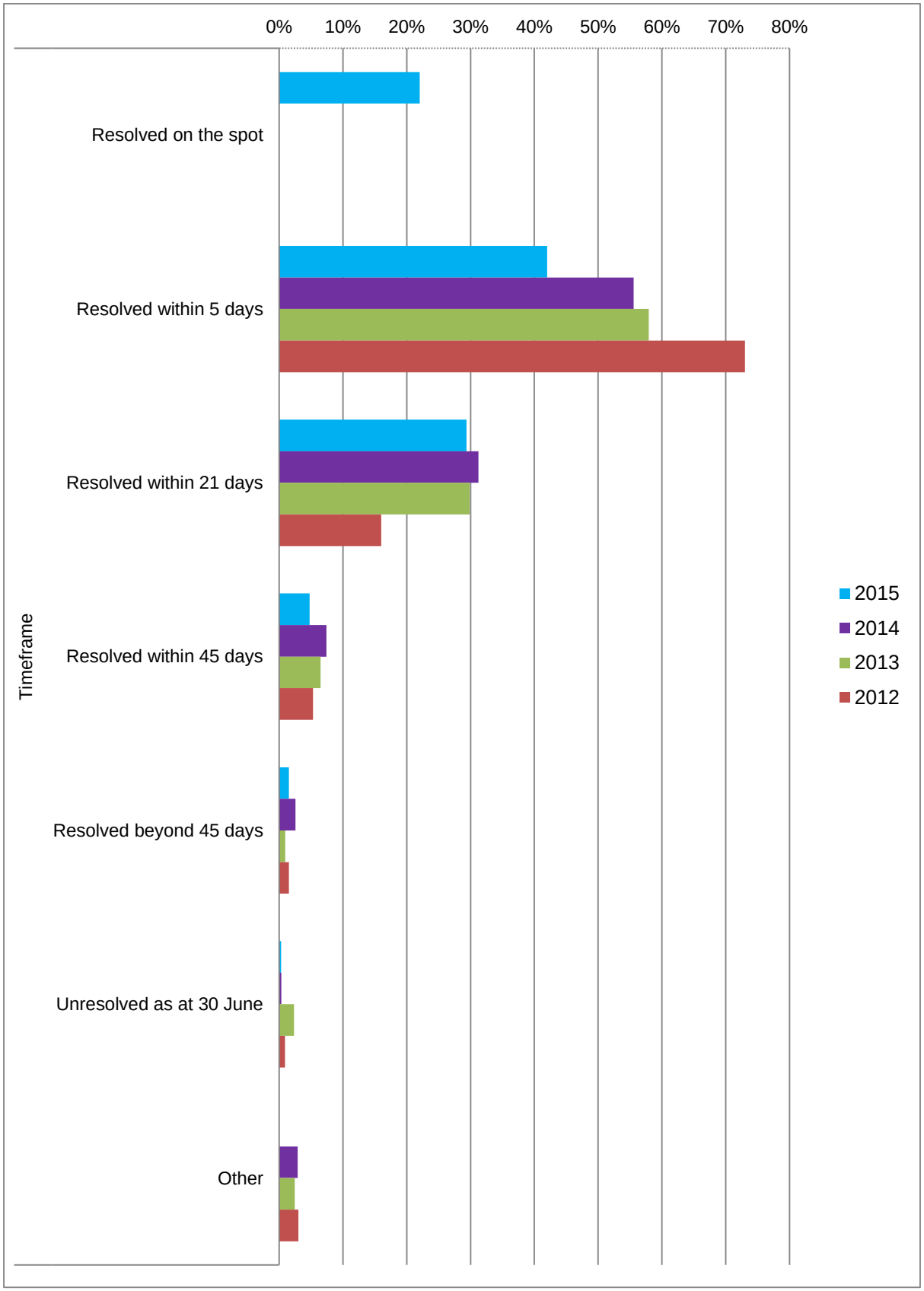
[6] 'Other' represents the number of complaints that were noted by the institution in the total number of complaints, but not further identified regarding the issue involved.

Chart 5: Percentage of complaints by outcome 2012–15[7]



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

Chart 6: Percentage of complaints by resolution timeframe 2012–15[8]



[8] 'Other' represents the number of complaints that were noted by the institution in the total number of complaints, but not further identified regarding the timeframe.

VERIFICATION PROGRAM

The 2014–15 Verification program tests and validates Code Subscribers' Code compliance programs, in particular how effectively they identified, reported and remedied breaches of the Code during the preceding 2013–14 period.

The Committee selected 14 Code Subscribers to take part in the program. Institutions were selected based on their 2014 ACS responses, where they showed signs of inconsistent or inaccurate complaints and breach data reporting. Participating institutions were geographically spread across the country and varied in size. The Verification program was conducted in February 2015 by telephone conferences.

Key issues

The key issues identified through the telephone conferences were the:

- inconsistent reporting of complaints and breaches, and
- missing link between the number of complaints reported in comparison to the number of Code breaches reported.

Only one of the 14 selected institutions reported that more than 1% of its customers raised a complaint between 1 July 2013 and 30 June 2014. Compared to the industry aggregate based on the complaints and breach data collected by the Committee over the past years, this appears to be very low:

	Average number of self-reported complaints per year based on data received since 2012	*Average number of self-reported Code breaches per year based on data received since 2011*
Small institution	12	2
Medium institution	75	10
Large institution	485	13

This indicates there may be an inconsistent approach to recording disputes/complaints and Code breaches among the participating institutions.

Some inconsistencies are based on:

EFT-, chargeback-* or *ATM-related disputes – some institutions reported that often these disputes are not considered as complaints about the institution, but directed against the relevant service providers. Institutions lodge the complaints with the service providers on behalf of their customers.

Financial difficulty hardship applications – some institutions considered that these were the only complaints that require follow up.

Resolved 'on the spot' – some institutions advised that they only record escalated complaints that required follow-up action. Complaints that are resolved by an explanation, apology, general discussion or acknowledgment of dissatisfaction are not recorded in their complaints register.

Source of breach data – some institutions advised referrals from staff and line managers are the main source of breach data. Other sources include internal audits, spot checks, social media such as Facebook and Twitter and disputes referred to the Financial Ombudsman Service Australia or the Credit and Investments Ombudsman. Despite this, 44% of the participating institutions recorded zero breaches in their 2013–14 ACS.

All participating institutions confirmed that they have in place a breach register, which is accessible to all staff. The common approach is for staff to record an 'incident' or 'event' in the breach register. The compliance manager or compliance team will then consult with the relevant line manager, legal team or senior management to determine whether an incident is considered a breach.

If a breach has been identified, the compliance manager or compliance team oversees the process in rectifying the breach. Remedial action often included remedial training for all staff or relevant teams.

As the number of complaints is directly correlated with the number of breaches, inaccurate complaints reporting has limited institutions' ability to identify Code breaches. As a result, institutions are not able to apply or test their breach procedures in practice.

To address these inconsistencies, the Committee encourages institutions to:

- review their definition of a complaint to include any expression of dissatisfaction made by the customer
- record all complaints in their complaints register including matters resolved 'on the spot'
- ensure that electronic funds transfer (EFT) and chargeback matters, ATM disputes and similar complaints are included in ACS complaints and breach data
- review their process to record and monitor Code breaches
- assess their link between complaints and Code breach reporting
- make Code breach reporting and complaints accessible to staff, and
- embed a positive reporting culture in the company's framework.

INVESTIGATIONS

The Charter empowers the Committee to receive any allegation from any person that a customer owned banking institution has breached the Code and to determine whether to investigate the matter. The Committee can also initiate its own investigations.

The Committee's investigations aim to identify the cause of alleged breaches and to make a determination whether there are broader compliance issues evident from the complaint and the effectiveness of remedial actions undertaken by institutions to minimise the impact of breaches on customers.

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 non-compliant behaviour identified through complaint investigations is systemic, either across an institution or the sector in general
- the presence of non-compliant behaviour that may not have been identified by the institution's internal compliance monitoring systems or its ACS, and
- emerging Code compliance risks that may affect a number of institutions and their customers.

Table 2: 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 customer potentially affected by the events.
☑ Assess if the breach is systemic and/or significant.
☑ Take remedial action to address the cause of non-compliance.
☑ Review and enhance processes and procedures.
☑ Train staff.

Investigations – case work

The Committee received two matters for investigation in 2014–15:

- one referral arising out of its engagement with consumer advocates, and
- one alleged breach of the Code, which was directly lodged with the Committee using the complaints form available through its website.

Alleged breach of Part C Key Promise 2 *'We will focus on our customers'*

Consumer advocates raised general concerns with the Secretariat regarding customer service standards when dealing with special needs customers.

Part C Key Promise 2 of the Code states that *'Our customer service standards will be appropriately tailored where we are aware that you have special needs (for example, because of your age or a disability, because you are an Indigenous person, because English is not your first language, or because you are unfamiliar with financial products and services).'*

The particular issues raised regarded:

- *Account opening fees* – the inability of customers to open a new bank account if they do not have access to sending money orders (for example if they live in remote areas) and have to send cash, which is not a preferred method as cash might get lost in the mail.

- *New key cards* – the inability of customers to order a new key card unless they have funds in the account to pay for a new key card.

- *Changes to processes regarding identification of an account holder* – customers are now asked up to nine questions regarding identification of an account. If customers are unable to answer these questions, they need to attend the local branch.

- *Overdrawn fees* – customers' accounts are overdrawn for several reasons, but there is no limit to the amount an account can be overdrawn (for example if the monthly overdrawn fee is charged to the account, but there is not enough money in the account, the customer will also get charged with the overdrawn/dishonour fee in addition to the monthly overdrawn fee, which puts the customer further behind).

- *Debit card* – consumer education by consumer advocates to apply for debit cards and not credit cards in order to only use money that they have is hindered by the process that debit cards require a customer assessment.

The Committee will assess future monitoring activities and stakeholder engagement in this area.

Alleged breach of obligations under Part D regarding disclosure of fees (Sections 4 and 5), financial difficulty assistance (Section 24) and debt collection (Section 26).

The online complaint stated that the institution was charging late payment fees on a home loan even though it was aware that the customer was in financial difficulty and despite the fact that the loan repayments, although late, were still being made in full.

The matter was closed when the customer did not provide the Committee with a privacy authority and further details so the Committee could engage with the institution about the matter.

Own Motion Inquiry (financial difficulty)

During 2014–15, the Committee conducted an inquiry to determine whether the practices of credit unions, mutual banks and mutual building societies were consistent with financial hardship provisions under the Customer Owned Banking Code of Practice.

While the Committee found the institutions surveyed were genuinely willing to help their customers in financial difficulty, they noted that obligations under the Code were broadly interpreted by institutions and not always consistently applied.

Most financial counsellors interviewed as part of the inquiry reported, for example, that some of the customers they represented were not offered a tailored or flexible repayment arrangement as would be expected. One-third of financial counsellors also reported instances where institutions had listed a default on their client's credit file or sold their debt while a request for financial hardship assistance was still being considered. This is again inconsistent with the Code's obligations.

The Committee highlighted three practices for particular attention:

- Code Subscribers should not pressure a customer to borrow from family and friends to pay out a debt or to access their superannuation early as this is inconsistent with the ASIC/ACCC Debt Collection Guidelines.

- Code Subscribers should review their procedures to ensure that they are not listing a default on a customer's credit reference file and will not sell the debt to a debt buy-out business while the institution is considering the customer's application or request, unless legally required to do so. These are obligations under the Code to which Code Subscribers must adhere.

- Code Subscribers should consider placing information on their websites to ensure consumers know where and how they can ask for assistance if in financial difficulty.

A full copy of the report is available at **http://www.cobccc.org.au/2015/01/30/reports-36-financial-difficulty-own-motion-inquiry-report/**.

Following the report's publication in January 2015, the Committee provided Code Subscribers with good practice guidance for compliance with financial difficulty obligations under the Code. An article was also provided to Consumer Federation of Australia (CFA) and Financial Council Australia (FCA) including a fact sheet for consumers outlining what to expect from an institution when experiencing financial difficulties, including:

- what assistance institutions can provide to customers experiencing financial difficulty
- what happens during the financial hardship application process
- where consumers can find financial difficulty information, and
- what consumers can do if their institution cannot assist.

ENGAGING WITH STAKEHOLDERS

In 2014–15, the Committee broadened its engagement with stakeholders to influence positive changes in industry behaviour, share industry experience of Code compliance and highlight areas of good industry practice.

Stakeholder liaison

The Committee and its Secretariat attended more than 25 meetings during the year involving ASIC, the Credit and Investments Ombudsman, Code Subscribers, consumer and small business representatives, and COBA.

Regulators

The Office of the Australian Information Commissioner (**OAIC**) invited the Committee to discuss the Own Motion Inquiry Report on Financial Difficulty, in particular the interaction between Code clauses 23.1 (*'Information privacy and security'*) and 24.2 *('If you are in financial difficulties'*).

The Secretariat also met with **ASIC** on various occasions to discuss the issue of direct debits cancellation fees, the impact of the Parliamentary Inquiry on ASIC's resourcing, the ASIC/ACCC Debt Collection Guidelines and the impact of a Federal Court decision in 2014 regarding responsible lending.

Consumer and small business representatives

The Secretariat collaborated closely with the Financial and Consumer Rights Council (**FCRC**) throughout the year. Staff members attended its compliance meetings, presented Code training sessions as part of the Council's Professional Development Program, and attended the FCRC annual conference in Creswick, Victoria.

Secretariat staff presented at the:

- National Conference of Community Legal Centres in Alice Springs
- Money Workers Association of the Northern Territory Conference in Alice Springs

- Financial Counselling Tasmania Annual General Meeting, and
- West Australian Financial Counselling Annual Conference in Perth.

Secretariat staff also attended the:

- Council of Small Business Australia (**COSBOA**) Small Business Conference in Melbourne
- Alzheimer Australia's NSW Conference regarding financial abuse of people with dementia
- Financial Counselling Australia's (**FCA**) Conference in Canberra, and
- ASIC Indigenous Super Summit in Melbourne.

These conferences provided a valuable opportunity to discuss Code compliance issues with financial counsellors and other consumer advocates and to understand trends in recent consumer experience of customer owned banking practice.

The Committee hosted a consumer advocate meeting in Sydney in February 2015 with representatives from Consumers' Federation of Australia (**CFA**), Financial Counselling Australia, Choice magazine and Financial Counsellors Association of NSW.

Code Subscribers

The Committee's engagement with Code Subscribers in 2014–15 focused on providing guidance on good industry practice, in particular compliance with financial difficulty obligations under the Code.

Publications

The Committee's website (**www.cobccc.org.au**) provides details of its role and functions and information about the Code, and reports on the work program. It also features an online form for individuals to report a concern that a Code Subscriber may have breached the Code and to identify any potential issues that may be emerging across the industry.

The Committee published:

- four editions of the *Accomplish* e-newsletter, keeping stakeholders up-to-date with activities and Code compliance news (edition numbers 20 to 23)
- an improved guide to codes of practice in conjunction with the Telecommunications Ombudsman and Energy and Water Ombudsman Victoria
- an updated *Code Toolkit*, a handy pocket-sized reference guide for financial counsellors
- four articles in the *FOS Circular* (August 2014, November 2014, January 2015, April 2015)
- an Own Motion Inquiry report on financial difficulty, and
- articles on financial difficulty for the CFA, FCA and Financial Planning Association of Australia (**FPA**).

2015–16 FUTURE OUTLOOK

The Committee will continue to work with Code Subscribers to improve standards of practice and service and share its experience of Code compliance. This will place the customer owned banking industry in a strong position to further increase customer satisfaction levels in the sector.

Code monitoring

The Committee will continue to work with COBA and Code Subscribers to ensure positive and consistent self-reporting of Code breach activity, and develop a risk assessment model to align Code monitoring activities with industry and other risk factors. This will include a benchmarking model for Code Subscribers to assess their performance against industry standards. Code Subscribers will also have improved access to information as part of the ACS program and Own Motion Inquiry via the online portal.

Investigations

The Committee will implement a streamlined process to ensure consistency, quality and continuous improvement of the Code function, including a review of the effectiveness and timeliness of decision-making processes and procedures. The Committee is currently developing guidance on the classification and enforcement of Code breach activity to ensure consistency and transparency of Committee decision-making. A guidance library is being developed for stakeholders about Committee operations and decisions.

Communication and engagement strategy

The Committee hopes to:

- review the content of the website to ensure it meets plain English benchmarks and stakeholder requirements
- work closely with COBA to develop a communications plan to enhance stakeholders' awareness of the Committee's operations and to reflect a common understanding of the roles of the Committee, and
- continue to provide consumer advocacy training and outreach programs with Ombudsmen schemes and compliance monitoring bodies.

APPENDIX A: Code Subscribers as at 30 September 2015[9]

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 Shoalhaven Community Credit Union
t/as Western City Credit Union
Community CPS Australia Limited
t/as Beyond Bank
Community First Credit Union Limited
Community Mutual Ltd
t/as Hunter Mutual
t/as New England Mutual
t/as Orana Mutual
Country First Credit Union Limited
Credit Union Australia Ltd
t/as CUA
Credit Union SA Limited
Dnister Ukrainian Credit Co-Operative Ltd
ECU Australia Ltd
EECU Limited
Encompass Credit Union Ltd
Family First Credit Union Limited
Fire Brigade Employees' Credit Union
Fire Service Credit Union Ltd
Firefighters & Affiliates Credit Co-operative Limited
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 Building Society Limited
Heritage Bank Limited
Heritage Isle Credit Union Ltd
Holiday Coast Credit Union Ltd
Horizon Credit Union Ltd
Hume Bank
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
Manly Warringah Credit Union Limited
t/as Northern Beaches Credit Union
Maritime Mining & Power Credit Union Limited
t/as Collie Miners Credit Union Ltd
t/as Reliance Credit Union
MCU Limited
mecu Limited
t/as Bank Australia
My Credit Union Limited
Northern Inland Credit Union Ltd
Nova Credit Union Limited
Old Gold Credit Union Co-operative Ltd
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
Qantas Staff Credit Union Ltd
QT Mutual Bank Limited
Quay Credit Union Ltd
Queensland Country Credit Union Limited
Queensland Police Credit Union Ltd
Queensland Professional Credit Union Ltd
t/as YCU Your Credit Union
Queenslanders Credit Union Limited
Railways Credit Union Ltd
Select Credit Union Limited
SGE Mutual Limited
t/as G&C Mutual Bank
Shell Employees' Credit Union Ltd
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 UniBank
The Broken Hill Community Credit Union Ltd
The Capricornian Ltd
Traditional Credit Union Ltd
Transcomm Credit Co-Operative 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

[9] The decrease in the number of Code Subscribers from 89 to 80 over the last 12 months follows a series of mergers and acquisitions within the industry and one cancellation of Code subscription.

APPENDIX B: Comparative table, self-reported Code breach data 2011–15

Group	Code category	2010/2011		2011/2012		2012/2013			2013/2014			2014/2015		
		Total		Total		Total		Sign[10]	Total		Sign	Total		Sign[11]
General	Key commitments (C1, C2, C7, C8, C9)	126	*30%*	42	*12%*	121	*13%*	3	129	*16%*	2	156	24%	1
	Provision of general information (D2, D19)	7	*2%*	29	*8%*	10	*1%*	1	21	*3%*	0	41	6%	1
	TOTAL GENERAL	**133**	*32%*	**71**	*20%*	**131**	*14%*	**4**	**150**	*18%*	2	**197**	**30%**	**2**
Disclosure	Interest rates, fees and charges (C3, D3, D5)	14	*3%*	27	*7%*	29	*3%*	2	65	*8%*	0	57	9%	0
	Terms and conditions (T&C) and changes to T&C (D4, D17)	24	*6%*	6	*2%*	35	*4%*	1	2	**[12]*	1	2	*	0
	TOTAL DISCLOSURE	**38**	*9%*	**33**	*9%*	**64**	*7%*	**3**	**67**	*8%*	1	**59**	**9%**	**0**
Provision of customer owned banking services	Account access and suitability (D13)	5	*1%*	4	*1%*	166	*18%*	0	84	*11%*	0	4	1%	0
	Account combination 'Centrelink requirements' (D26.4)	0	*0%*	0	*0%*	1	*	0	1	*	0	0	0%	0
	Direct debit arrangements (D20)	15	*4%*	28	*8%*	15	*2%*	0	9	*1%*	0	4	1%	0
	Recurring payment arrangements (D20.3)[13]	0	*0%*	0	*0%*	2	*	0	3	*	0	3	*	0
	Chargebacks (D21)	8	*2%*	0	*0%*	151	*16%*	0	172	*22%*	0	0	0%	0
	Statements of account (D16)	11	*3%*	10	*3%*	13	*1%*	1	11	*1%*	0	21	3%	1
	TOTAL PROVISION OF CUSTOMER OWNED BANKING SERVICES	**51**	*10%*	**42**	*12%*	**348**	*37%*	**1**	**280**	*35%*	0	**32**	**5%**	**1**
Provision of credit	Credit assessment (C4, D6, D7)	9	*2%*	3	*1%*	9	*1%*	1	13	*2%*	0	17	3%	0
	Financial difficulties (D24)	0	*0%*	3	*1%*	2	*	0	3	*	0	1	*	0
	Joint debtors, joint accounts and subsidiary	4	*1%*	2	*1%*	1	*	0	0	*0%*	0	0	0%	0

[10] Sign = Significant breaches (first requested for this report in 2012–13).
[11] For details see Appendix C.
[12] * Not shown as percentage is below 1%.
[13] Prior to 1 January 2014 this category refers to section D20.3 of the 2010 Mutual Banking Code of Practice.

	cards (D9, D10, D11)													
	Reverse Mortgage Loans (D8)	0	*0%*	0	*0%*	0	*0%*	0	0	*0%*	0	0	0%	0
	Guarantees (D12)	3	*1%*	3	*1%*	2	*	0	0	*0%*	0	1	*	0
	Debt collection (D26)	4	*1%*	1	*	2	*	0	3	*	0	1	*	0
	TOTAL PROVISION OF CREDIT	**20**	*5%*	**12**	*4%*	**16**	*1%*	**1**	**19**	*2%*	0	**20**	**3%**	**0**
Training, Privacy, IDR and other	Privacy and security (D23)	93	*21%*	97	*26%*	111	*12%*	1	105	*13%*	1	129	20%	2
	Advertising (D1)	12	*3%*	23	*6%*	34	*4%*	1	10	*1%*	1	13	2%	0
	Closure of accounts (D22)	3	*1%*	2	*1%*	2	*	0	4	*1%*	0	1	*	0
	Communication (D15, D18, D25)	5	*1%*	5	*1%*	21	*2%*	0	23	*3%*	1	27	4%	0
	Training (C5, D14, E2)	29	*7%*	28	*8%*	170	*20%*	0	132	*17%*	0	165	26%	0
	Dispute resolution (C6, D27, D28, D29, D30)	44	*11%*	42	*12%*	15	*2%*	0	5	*1%*	0	3	*	0
	Promotion of Code (B, C10, E1)	3	*1%*	9	*2%*	5	*1%*	5	5	*1%*	0	0	0%	0
	TOTAL TRAINING, PRIVACY, IDR and OTHER	**177**	*44%*	**206**	*55%*	**358**	*41%*	**7**	**284**	*36%*	3	**338**	**52%**	**2**
TOTAL		419		364		917		16	800		6	646		5
Number of institutions that reported breaches		44	*44%*	50	*53%*	56	*62%*	9	50	*56%*	5	49	61%	5

APPENDIX C: Examples of self-reported Code breaches in 2014–15

Breach details	*Remedial actions*
GENERAL COMMITMENTS	
Key commitments (C1, C2, C7, C8, C9)	
Breaches for C2 referred to staff members not dealing appropriately with customers. A staff member failed to follow customer management protocols. Problems arose with a difficult customer in unusual circumstances. On investigation it was determined the customer's issues could have been better managed.	The staff member received counselling. Customer management protocols were reviewed to provide guidance to staff and additional staff training was provided on these protocols.
Breaches for C8 involved staff members not completing verification processes before providing deposit services. In both cases the customers were known but the necessary information requested had not been received in a timely fashion. The staff member's provision of assistance to the customers was at the expense of regulatory compliance.	Staff received counselling.
E-payment timeframes were exceeded. This was caused by staff not understanding implications of public holiday inclusions.	Staff are now aware of requirements.
Electronic funds transfers (EFTs) were delayed.	Better processes and controls have been put in place so this does not reoccur.
Provision of general information (D2, D19)	
Multiple breaches occurred in the contact centre with staff not fully reading scripts, resulting in some product information being missed.	Coaching was provided to staff in all cases and, where appropriate, the customer was phoned back to provide the information.
The breach was in relation to a minor omission from part of a disclosure for a printed home loan ad.	The online version was amended. The omission was not considered misleading.
DISCLOSURE	
Interest rates, fees and charges (C3, D3, D5)	
Relevant credit card warning details on statements were missing for one month. Relevant transaction fee table disclosures were missing from same month's statement run. This was caused by a combination of system upgrades and mail-house changes.	Information was corrected for the next statement run. New checklists were produced for future upgrades.
Issue with clear information.	The website was updated to include clear and accurate information and instructions. Both staff and customers can readily access this information when required.
Incorrect system generated Late Payment Fee being charged.	Investigation completed. Only a limited number of customers were impacted. As a result of the investigations, documentation has been updated to reflect that the institution does not charge a

Breach details	*Remedial actions*
	Late Payment Fee – only enforcement fees are charged.
Solutions Home Loans Annual Fee not charged correctly.	Investigation completed. The program has been deactivated and annual fees will be charged manually until a system fix is implemented. Adjustments have been processed regarding any over / under charges to customers.
The Term Deposit rate schedule had not been updated on the institution's website.	The advertised rate was honoured. Controls/procedures were implemented to ensure no reoccurrence. Staff training was provided.
PROVISION OF CUSTOMER OWNED BANKING SERVICE	
Account access and suitability (D13)	
Third party businesses that contributed to a customer complaint assisted the institution with an investigation to understand the circumstances that led to the customer's dissatisfaction.	Where applicable, a fix was implemented, and the outcome and/or apology were communicated to the customer.
Statements of account (D16)	
A 'Statement Fee Table' was not being produced on statements where there was a change in a product type. This affected three customers.	This issue was detected as part of the institution's due diligence testing. It was rectified in a timely manner.
Multiple 'Statement Fee Tables' appeared on statements. Customers were not impacted from a monetary perspective, and the amount of fees charged and processed to the accounts were correct and were correctly stated on each statement. However, information in the Statement Fee Tables may have been confusing to customers.	No customer complaints were received and the matter was resolved. Further testing was undertaken to ensure this would not reoccur.
Following a fee restructure, two months' worth of customers' monthly account statements did not disclose transaction fees broken down by transaction type, but were instead bundled as one transaction fee total.	Statement templates were reviewed and corrected to ensure that the prescribed fee disclosure breakdown was included, and ongoing testing arranged to ensure correct disclosures continue.
TRAINING, PRIVACY, IDR & OTHER	
Communication (D15, D18, D25)	
Issue: electronic communication.	An investigation was completed to determine the cause of a process failure. Once the problem was understood, new instructions were communicated to staff to enable them to assist customers.
Issue: timely, clear and effective communication.	Staff members responsible for breaches received counselling.
The breach related to communication of a branch relocation. Customers were notified in newsletters and via the website, however,	Reviewed communication processes to customers.

Breach details	*Remedial actions*
some customers would prefer written personal information.	
Dispute Resolution (C6, D27, D28, D29, D30)	
The issue concerned premiums on home and contents insurance with 'flood cover', with the institution acting as agent for the insurer. An issue arose where a customer compared premiums with another customer who lived in a similar area and complained that his premiums were too high.	The matter was referred to the insurer who refunded the customer in good faith and the matter was closed.
A customer was not informed of the need for an extension of the 21-day timeframe for resolving their complaint.	A letter was sent to the customer advising of the extension and the staff member involved was counselled.
The issue concerned oversight by a staff member when dealing with a one-off complaint; the staff member failed to inform the customer of the EDR scheme.	The complaint was resolved in the customer's favour. This failure was an oversight; the staff member was advised. Changes to the controls were not required.
Privacy & Security (D23)	
Breaches related to information/card being sent to an incorrect address and to a signatory on one sub-account being provided deposit transaction information on a sub-account to which they were not a signatory.	Staff coaching was provided and affected customers were contacted.
Privacy breaches have been attributed to a number of different channels: • mailing house folding statements together • operator issuing visa debit card to the incorrect customer, and • internet banking password given to an ex-customer to an account in error.	With all occasions, the issue was handled swiftly. A full investigation was undertaken to confirm where the system had failed and training was undertaken with individuals.
Faxes were sent to the incorrect customers.	Staff were reminded to check the information that they are faxing, to ensure that the correct information is being sent to the right people.
The staff member did not identify the customer correctly and presumed that the customer they were serving was the person who owned the account. Information was given to that person who was not the signatory on the account.	The staff member concerned was given extra training.
The staff member spoke with a customer on an account, who had incorrectly been added to the account, and gave them information.	Staff were stressed the importance of checking their work and ensuring that they check what they have inputted.
An account opening letter was sent to an unintended customer.	The customer was contacted, advised of the breach, the account closed and a new one opened with the staff concerned counselled.
One instance concerned a manual error with an incorrect customer's address entered onto correspondence resulting in the customer's personal account information being distributed to the wrong customer.	The circumstances surrounding each breach were unique and not related. Controls were introduced to prevent recurrence, including review of relevant processes and systems and counselling of staff.

Breach details	*Remedial actions*
One instance concerned an external mail-house error resulting in two customers' term deposit renewal letters being sent to one customer in the one envelope. The third instance involved a banking system improperly retaining personal information relating to online applications, which was not destroyed or de-identified when the applicants did not become customers.	
A First Home Savers Account annual statement was sent to the wrong address.	The breach was rectified and the correct statement resent to the correct address.
Customer complaint due to breach of privacy.	Investigation completed. Sent a response to the customer and sought legal advice. No regulator notification required.
Information about a customer's account that was intended for staff eyes only via email, was accidentally sent to an external party unrelated to the account.	The breach was actioned by reporting it to the Breaches Report, conducting a staff training session and notifying all affected parties immediately. The affected customer was satisfied that the breach has been attended to.
Unrelated privacy incidents, rated as insignificant and not systemic in nature. The increase in reported breaches from the previous period is primarily attributable to revision of the Privacy Act in March 2014, which provided a timely reminder to staff of their obligations under the Act and the new rules, appearing to have prompted more proactive reporting of breaches.	The breaches were addressed following each occurrence by raising staff awareness and refresher training being provided to impacted staff on privacy obligations. In response to the increase in reported privacy breaches, a refresher communication is being developed along with guidelines and frequently asked questions to assist staff to understand and comply with privacy requirements.
Tax file numbers (TFNs) were not deleted after being scanned as per TFN guidelines.	A software enhancement has automated this process.
Promotion of the Code (B, C10, E1)	
Website not up-to-date.	The institution’s website being updated to include link to the Code with ability to download booklet.
Training (C5, D14, E2)	
A number of breaches occurred at the supplier end.	Appropriate actions or Service Level Agreements are now in place plus internal procedures to monitor.
Customer service standards were inadequate.	Internal counselling and/or remedial training was provided, as considered appropriate, to the staff members of concern.
Christmas Club funds were not available on the specified date.	This was caused by a system issue that has now been rectified.

APPENDIX D: Significant breaches self-reported in 2014–15[14]

Key commitments KP8 *'We will comply with our legal and industry obligations'*	
Issue	Customers were identified that should have received a bonus interest on their 'Bonus Saver' accounts but were only paid the base rate of interest. Over a six-month period (1 March – 31 August 2014) some customers were underpaid on more than one occasion.
Background	The cause of this particular issue was a misunderstanding between Marketing and the Technology departments. A flawed interpretation of the operation of the system by Technology resources led them to conclude that there would be no need for a system change to accommodate the new product feature, when this was not in fact the case. Affected customers that were eligible for the 'bonus' interest were only paid the (lower) "base" rate of interest. While the impact to approximately 83% of the affected customers was less than $10 over the six-month period, it was the institution's view that given the systemic nature of the issues, the overall affected class by number, and the fact that some customers were impacted on more than one occasion, and some by in excess of $100, that this constituted a significant breach.
Outcome	A significant breach was reported to ASIC along with a rectification plan to resolve the breach and mitigate against a recurrence of this issue. The rectification plan included issuing a letter to all impacted customers notifying them of the matter, making interest adjustments to the impacted customers, and developing system changes necessary to address this issue on a permanent basis. Regular written progress updates were provided to ASIC reporting on the institution's execution of the rectification plan, and all of the actions outlined in the plan were completed within the timeframes committed to ASIC and fully resolved on 1 December 2014. ASIC provided final written correspondence to the institution on 13 January 2015 advising that it was satisfied with the remediation of the breach, and that it did not intend to take any further action in relation to this matter.
Provision of general information D2 'Information about our products'	
Issue	Institution changed third-party insurance partner. During this process it was identified that a subset of customers purchasing insurance were not being issued with the Financial Services Guide (FSG) from the new insurance partner.
Background	Institution determined this to be a material breach of its obligations, specifically section 941 of the Corporations Act. ASIC was notified under section 912D and a remediation plan was agreed and implemented. ASIC was satisfied with the institution's response to the incident, including the agreed remediation plan.
Outcome	Remedial action agreed was as follows: Phase A: Immediate response: 1. Identify affected customers and issue them a correct FSG with an explanatory letter. This letter to include an offer of premium refund to customers who had not claimed on their policies.

[14] In order to ensure de-identified information, any reference to the number of affected customers and details of products has been removed.

	2. Implement interim processes to ensure all future insurance customers were provided with the FSG. This included scripting for staff and introducing a back-end process to manually mail FSGs to relevant customers. Phase B: Further improvements 3. Complete sales process mapping for all products and channels, including mapping required for regulatory disclosures. 4. Conducting an internal audit of the insurance sales process. 5. Additional staff training on processes. 6. Engaging external consultant to undertake an external Compliance Maturity Review of third-party product's compliance arrangements generally. 7. Implementing 2nd Line compliance assurance activities. 8. Reviewing and updating management processes.
Provision of customer owned banking services D16 *'Account statements and balances'*	
Issue	Statements of accounts: D16 'account statements and balances' – one significant breach of D16.2 whereby minimum prescribed repayment warnings were not correctly included on monthly Visa Card account statements as specified in s79B of the *National Consumer Credit Protection Regulations 2010*. Missing information was not disclosed between September 2012 and August 2014. This breach was reported to ASIC on 26 September 2014.
Background	The system flag, which automatically generates the required information, had defaulted to 'N' and the information stopped generating on credit card statements from September 2012. A breakdown in controls surrounding statement validation, after they had been generated but before they had been issued by the mail-house, also resulted in this error.
Outcome	The breach was assessed as significant and reportable to ASIC on the basis that credit card customers were potentially impacted and the incomplete minimum repayment warning disclosure had continued between September 2012 and August 2014. The institution had not been in receipt of any customer complaints about this matter and is not aware of any credit card customers having been adversely impacted by the incomplete disclosure. Full minimum repayment warning disclosure has been displayed on all credit card statements from September 2014. Periodic testing is being performed on monthly credit card and account statements to ensure correct disclosures are being made. All credit card customers were advised of the error as part of their October 2014 credit card statement. Enhanced system controls have been implemented including approvals required for any future changes made within the systems program to the credit card statement template.
Privacy & security D23 *'Information privacy and security'*	
Issue	Privacy notification forms were not being supplied to new customers when opening accounts
Background	Privacy notification forms were not being included in new account opening packs.
Outcome	Legal action was obtained. The form was sent to all customers when a full statement run was completed. Instructions were sent to all staff who prepared the packs with a pro-forma document stating what documents had to be included in the pack. Compliance Manager checks a sample of packs each month to ensure that they contain the correct forms.

Privacy & security D23 *'Information privacy and security'*	
Issue	Staff member became aware that they had been recording the Privacy Act requirement, 'Opt-out' flag incorrectly. Investigation determined that the error had been occurring since 2010.
Background	The Application for membership asks the member if they wish to 'opt-out' of receiving marketing material. The Customer Information System database records if the member wishes to receive marketing material. The guidance material was not clear enough to ensure the two were not confused.
Outcome	Records have been checked from hardcopy applications to the database and corrected where required. Management action in the form of checking the application to the database to ensure the flag is appropriately recorded is now required. Procedures relating to this process have been reviewed and updated to ensure clarity.

APPENDIX E: Comparative table, self-reported IDR data 2011–15

	Category	2011/2012		2012/2013		2013/2014		2014/2015	
Products/ services involved in consumer complaint	Consumer Credit Insurance	0	*0%*	13	**[15]*	17	*	**36**	*0%*
	Credit	1,299	*12%*	448	*3%*	511	*4%*	**445**	*3%*
	Deposit Taking	3,345	*32%*	2,166	*15%*	1,829	*15%*	**1,930**	*12%*
	General Insurance	140	*1%*	132	*1%*	180	*1%*	**263**	*2%*
	Investments	145	*1%*	26	*	59	*	**219**	*1%*
	Life Insurance	36	*	13	*	5	*	**0**	*0%*
	Mortgage	0	*%*	530	*4%*	414	*3%*	**661**	*4%*
	Payment Systems	2,232	*20%*	6,334	*44%*	4,075	*33%*	**3,746**	*22%*
	Personal Loan	0	*0%*	350	*1%*	377	*3%*	**449**	*3%*
	Small Business Loan	0	*0%*	4	*	6	*	**17**	*
	Superannuation	0	*0%*	3	*	9	*	**11**	*
	Traditional Trustee Services	0	*0%*	0	*0%*	4	*	**6**	*
	Other[16]	3,204	*31%*	4,374	*30%*	4,923	*40%*	**8,926**	*53%*
Issues involved in customer complaint	Advice	94	*1%*	84	*1%*	100	*1%*	**413**	*2%*
	Charges	907	*9%*	1779	*12%*	2,026	*16%*	**4,792**	*29%*
	Disclosure	628	*6%*	211	*1%*	211	*2%*	**279**	*2%*
	Financial Difficulty	76	*1%*	78	*1%*	122	*1%*	**109**	*1%*
	Decision by institution	0	*0%*	239	*2%*	383	*3%*	**565**	*3%*
	Instructions	236	*2%*	517	*4%*	903	*7%*	**624**	*4%*
	Privacy	87	*1%*	140	*1%*	121	*1%*	**103**	*1%*
	Responsible Lending	0	*0%*	15	*	35	*	**65**	*
	Service	3,287	*32%*	4,752	*33%*	4,822	*39%*	**3,083**	*18%*
	Transactions (incl ATM issues)	4,325	*42%*	3,859	*27%*	2,291	*18%*	**3,104**	*19%*
	General feedback or improvement suggestion	n/a	n/a	n/a	n/a	n/a	n/a	**2,259**	*14%*
	Other	761	*7%*	2,719	*19%*	1,395	*11%*	**1,313**	*8%*
Outcome of customer complaint	In favour of customer	4,164	*40%*	3,935	*27%*	4,371	*35%*	**6,022**	*36%*
	In favour of institution	1,833	*18%*	1,181	*8%*	1,335	*11%*	**822**	*5%*
	Customer taken legal action	0	*0%*	1	*	1	*	**8**	*
	Mutual agreement	2,547	*24%*	6,812	*47%*	5,941	*48%*	**3,228**	*19%*

[15] * Not shown as percentage is below 1%.
[16] 'Other' represents the number of complaints that were not further specified by institutions.

	Category	2011/2012		2012/2013		2013/2014		2014/2015	
	Referred to External Dispute Resolution	149	*1%*	206	*1%*	92	*1%*	**177**	*1%*
	Withdrawn	12	*	322	*2%*	199	*2%*	**119**	*1%*
	Apology, explanation and/or acknowledgement of feedback	n/a	*n/a*	n/a	*n/a*	n/a	*n/a*	**5,675**	*34%*
	Other	1,654	*16%*	289	*2%*	425	*3%*	**608**	*4%*
	Outstanding	42	*	1,647	*11%*	45	*	**50**	*
Timeframe	Resolved on the spot	7,713	*73%*	8,338	*58%*	6,894	*56%*	**3,681**	*22%*
	Resolved within 5 days	7,713	*73%*	8,338	*58%*	6,894	*56%*	**7,016**	*42%*
	Resolved within 21 days	1,583	*16%*	4,299	*30%*	3,834	*31%*	**4,909**	*29%*
	Resolved within 45 days	552	*5%*	932	*6%*	920	*7%*	**797**	*5%*
	Resolved beyond 45 days	159	*2%*	135	*1%*	317	*3%*	**256**	*2%*
	Unresolved as at 30th June	94	*1%*	337	*2%*	45	*	**50**	*
	Other	300	*3%*	352	*2%*	359	*3%*	**0**	*0%*
Number of complaints which include Code breaches		117	*1%*	309	*2%*	370	*3%*	**233**	*1%*
Total number of complaints		10,401		14,393		12,409		**16,709**	
Number of institutions that reported complaints		67	*71%*	82	*90%*	79	*89%*	**70**	*88%*

APPENDIX F: Additional tables, complaints & breach data 2011–15

Number of customer complaints and Code breaches by size of institution

	Number of complaints					Number of Code breaches				
	2011[17]	2012	2013	2014	2015	2011	2012	2013	2014	2015
Total number of institutions	n/a	95	91	89	80	99	95	91	89	80
Reported by all institutions	n/a	10,401	14,393	12,409	16,709	419	364	917	800	646
Reported by institutions with - over 100 FTE[18]	n/a	8,829	11,292	9,732	14,107	199	236	287	269	447
- 31 to 100 FTE	n/a	1,377	2,552	2,191	1,970	169	84	520	455	119
- up to 30 FTE	n/a	195	549	486	632	51	44	110	76	80

Number of institutions reporting complaints for period 2011–2015

	Number of institutions				
Number of reported complaints	2011	2012	2013	2014	2015
Nil	n/a	23	9	10	10
Between 1 to 10	n/a	25	23	29	18
Between 11 to 20	n/a	15	13	14	8
Between 21 to 50	n/a	7	18	10	17
Between 51 to 100	n/a	6	8	6	6
Over 100	n/a	14	20	20	21
Not advised	n/a	5	0	0	0

Number of institutions reporting Code breaches for period 2011–2015

	Number of institutions				
Number of reported Code breaches	2011	2012	2013	2014	2015
Nil	46	40	35	39	31
Between 1 to 10	37	41	39	32	33
Between 11 to 20	3	6	7	10	5
Between 21 to 50	2	2	7	6	9
Between 51 to 100	1	1	2	1	2
Over 100	1	0	1	1	0
Not advised	9	5	0	0	0

[17] The 2011 Annual Compliance Statement did not request customer complaints data for 2010–11.
[18] FTE = full time equivalent employees.