



CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

Annual Data Report 2021-22

**Findings from breaches
and complaints to
achieve better
customer outcomes**

April 2023

cobccc.org.au

***We acknowledge the traditional custodians of the different lands across Australia,
and pay respects to elders past, present and future.***

*For they hold the songlines
The stories
The traditions
The culture
And the hopes of First Nations Australia.*

This land is, was, and always will be traditional First Nations country.

*We also acknowledge and pay respects to the traditional custodians of the lands on which
we work: the Wurundjeri, Boonwurrung, Wathaurrung, Daungwurrung and Dja Wrung
peoples of the Kulin nation and the Gadigal people of the Eora Nation.*

Contents

CONTENTS	3
CHAIR'S MESSAGE.....	4
INTRODUCTION.....	6
THE SECTOR – A SNAPSHOT.....	7
BREACHES – A SNAPSHOT.....	8
KEY INSIGHTS.....	11
Quality of reporting needs improvement	11
Categorising breaches for meaningful insights	11
Facing challenges.....	13
Increase in reported complaints	13
Looking ahead.....	14
BUSTING MISCONCEPTIONS	15
DATA ANALYTICS.....	17
Part A: Details of Code subscribers	17
Part B: Breach data.....	19
Part C: Complaints data	26
Part D. Data trends.....	28
Part E. Breach data of the past five years	30
Part F. Complaints data of the past five years.....	34
Breaches by specific Code obligations.....	38
About the Code	39
About the Committee.....	39

Chair's message

As Chair of the Customer Owned Banking Code Compliance Committee (COBCCC), I am pleased to present the 2021–22 Annual Data Report.

The data tells us a lot about the successes and challenges for subscribers during the reporting period.

Reporting and not enough reporting

First, I want to acknowledge the subscribers that reported breaches and complaints for the period.

This demonstrates that subscribers have compliance frameworks, systems and processes in place for recording and reporting breaches and complaints.

Reporting breaches and complaints is not simply an exercise in meeting administrative obligations. Taken seriously, and done properly, it provides a way to understand and address issues and identify areas of concern. And this is fundamentally important for any institution with a desire to improve and bring about good customer outcomes.

Unfortunately, however, 2021-22 also saw some subscribers report very few or no breaches and some report very few or no complaints.

Reporting very few or nil complaints or breaches is not normal and brings into question a subscriber's monitoring and reporting systems and capabilities.

Insufficient monitoring and reporting capabilities might suggest poor practices and governance. It reveals an institution yet to embrace a culture of compliance.

Monitoring, identifying and reporting breaches and complaints is an integral obligation of any financial services organisation and is part of improving services and outcomes.

All subscribers should have a culture of compliance and work to make sure the Board and all staff understand its benefits – it exists to properly monitor compliance, identify and report breaches, remediate when required and learn from them.

We have included a section on Busting Misconceptions on pages 15 and 16 of this report to provide further insights on the misconceptions that the Committee believes lead to under reporting of breaches and complaints by subscribers.

This will be an area of focus for the Committee in the coming year.

Being specific when reporting breaches

We found that too many subscribers reported breaches under Key Promises instead of the more specific, and more appropriate, provisions of the Code related directly to the breach.

Not assessing breaches thoroughly and classifying under the general Key Promises fails to provide vital information about the nature of the breach. This necessarily places a limit on what a subscriber – and the industry more broadly – can learn from the breach.

We expect to see subscribers using specific Code provisions when reporting breaches.

This helps identify the cause of a breach and helps a subscriber address the issue and undertake effective remediation. It also helps generate quality data and insights.

Reporting breaches is good, but it is only half the job. It is important to make sure the reporting is specific and provides the information required for insights.

Challenges

The ACS Verification Program provided us with valuable insight into the challenges that subscribers faced in 2021-22.

Evidently, staffing and resourcing continues to be an issue for customer owned banking institutions.

Regulatory change, as well as the introduction of the new Code, also posed some challenges in 2021-22.

ASIC's [Regulatory Guidance 271 – Internal Dispute Resolution](#) came into effect, requiring subscribers to comply with its provisions for internal dispute resolution and recording and reporting complaints.

The new product [design and distribution obligations](#), which require subscribers to design financial products to meet the needs of consumers and be more targeted with distribution, also placed considerable pressure on subscribers.

Of course, the new Code featured among all this too.

Transitioning to the 2022 Code required subscribers to enhance compliance frameworks and implement necessary changes and upgrades.


We recognise the resources required for such work and, as the Committee, we appreciate the efforts we saw from most subscribers.

As the dust settles on the implementation of the 2022 Code, we are confident that most subscribers have prepared well and will continue to prioritise compliance. We look forward to the results in the coming months and years.

Thank you

I would like to thank my Committee colleagues, Cindy Hansen and Philip Cullum, for their work throughout the year.

Also, a sincere thank you to our Code team at AFCA for the wonderful support role it plays. The team has worked tirelessly during the year in assisting us carry out our role of monitoring compliance with the Code.



Jocelyn Furlan
Independent Chair
Customer Owned Banking Code Compliance Committee

Introduction

The 2021-22 Annual Data Report provides analysis on breaches of the Customer Banking Code of Practice (the Code) and complaints reported to us by subscribers to the Code for the reporting period of 1 July 2021 to 30 June 2022.

The Annual Data Report is a companion report to our [2021–22 Annual Report](#) and includes our observations on compliance with the Code, along with guidance for subscribers that will help them improve and achieve better practices.

Methodology

One of the main ways we monitor compliance with the Code is through the Annual Compliance Statement (ACS). Code subscribers must provide detailed data about their breaches and the total number of complaints annually in the ACS, each time reporting on the preceding twelve-month period.

As part of the 2021-22 ACS, 55 Code subscribers provided data on their breaches and complaints.

We also contacted all subscribers to clarify their data or if they had unusual reporting patterns (for example, no reported breaches, a high number of breaches, or breaches that affected high numbers of clients).

The findings are drawn from the ACS data, as well as insights and lessons drawn from calls with subscribers.

Transition to the 2022 Code

The new 2022 Code came into effect 31 October 2022.

Although the data in this report covers the twelve months period until 30 June 2022 when subscribers self-reported against the 2018 Code, we have included reference to the 2022 Code in the data collection to help subscribers transition to the 2022 Code.

We took a thematic approach which gave subscribers the opportunity to report against either version of the Code and analyse their data by theme.

The sector – a snapshot

Note: Numbers as at 30 June 2022. Comparisons are with the 2020-21 financial year.



55 SUBSCRIBERS

Down from 57 in 2020-21, due to mergers. See the [full list of subscribers](#) at the COBA website

644 BRANCHES



Down from 793 in 2020-21.

9,600 EMPLOYEES



Down from 9,430 in 2020-21.

STRONG PRESENCE IN REGIONAL AUSTRALIA - 8 OF THE 10 LARGEST CODE SUBSCRIBERS HAVE HEAD OFFICES OUTSIDE SYDNEY & MELBOURNE



3.6 MILLION MEMBERS



Down from 3.8 million in 2020-21.



9.1 MILLION ACCOUNTS

Up from 8.6 million in 2020-21.

MEMBERS MAKE UP 14% OF AUSTRALIA'S POPULATION

BREAKDOWN OF SUBSCRIBERS

Category	Subscribers		Branches		Members		Accounts	
CAT AA (Assets > \$5B)	9	↑ 1	296	↓ 2	2.3M	↓ 4.7%	5.2M	↑ 0.2%
CAT A (Assets \$2B - \$5B)	6	↓ 1	130	↓ 4	530K	↓ 13.4%	2.1M	↑ 41.0%
CAT B (Assets \$1B - \$2B)	11	=	96	↓ 135	430K	↓ 3.0%	1.1M	↓ 8.3%
CAT C (Assets \$500M - \$1B)	9	↑ 1	57	↑ 4	186K	↑ 13.1%	372K	↑ 5.2%
CAT D (Assets \$200M - \$500M)	11	=	43	↑ 1	111K	↑ 1.8%	191K	↓ 5.3%
CAT E (Assets < \$200M)	9	↓ 3	22	↓ 13	60K	↓ 33.8%	140K	↓ 10.2%

Note: Comparisons with the 2020-21 reporting year.

Breaches – a snapshot

A BREACH IS A FAILURE TO COMPLY WITH THE OBLIGATIONS OF THE CODE IN RELATION TO THE PROVISION OF A CUSTOMER OWNED BANKING SERVICE.

(Defined with reference to ASIC Regulatory Guide 78 – Breach Reporting by AFS Licensees, [Standards Australia's AS 3806-2006](#) – Compliance Programs, and [Section 912D of the Corporations Act 2001](#)).

REPORTED BREACHES & SUBSCRIBERS OVER THE YEARS

Aside from the Covid-affected year of 2020-21, breaches have steadily increased. Over the same period, the number of subscribers has fallen as a result of mergers.



4 SUBSCRIBERS CHOSE TO REPORT BREACHES UNDER THE 2022 CODE IN 2021-22

We congratulate these subscribers on implementing the new Code into their processes and procedures before it became effective on 1 November 2022.

SUBSCRIBERS ATTRIBUTED BREACH INCREASES TO...

- review of systems and processes for the 2022 Code
- increased awareness of the Code
- improved guidance and staff training
- increased engagement with the COBCCC on reporting



IN THE 2021-22 REPORTING PERIOD, WE FOUND...



13% INCREASE

IN TOTAL SELF-REPORTED BREACHES

↑ Increase in breaches of all but two sections in the Code

= No change in reported breaches of 'Key Promises'

↓ Decrease in breaches of 'Approach to lending' obligations

OF 55 SUBSCRIBERS, 42 (76%) REPORTED BREACHES IN 2021-22

**22 SUBSCRIBERS REPORTED AN
INCREASE IN BREACHES**

**20 SUBSCRIBERS REPORTED A
DECREASED IN BREACHES**



13

SUBSCRIBERS REPORTED NO BREACHES

The same subscribers that reported no breaches in 2020-21: six from Category E, six from Category D, one from Category C

THE MOST COMMON BREACHES

	Code Section	Breaches	Notes
1	Key Promises	894 (↓ 5)	50% related to Key Promise 5 of the 2018 Code
2	Privacy obligations	811 (↑ 52)	99% related to D23 of the 2018 Code
3	Interest rates, fees & charges	186 (↑ 73)	97% related to D3 and D5 of the 2018 Code
4	Provisions for product information	159 (↑ 50)	94% related to D2 of the 2018 Code
5	Lending obligations	72 (↓ 70)	97% related to D6 of the 2018 Code
6	Training obligations	64 (↑ 60)	91% related to B13 of the 2022 Code
7	Communication obligations	54 (↓ 21)	68% related to D15 of the 2018 Code, 32% related to B15 & B16 of the 2022 Code

Note: Figures in brackets are the differences with the breaches reported in the 2020-21 reporting year.

THE IMPACT...



**BREACHES IN 2021-22 HAD
A FINANCIAL IMPACT OF**

\$33.67M

Up from \$9.07 million in 2020-21.

HOWEVER...

A single breach accounted for \$28.9 million of impact. This breach, which affected 126 customers, related to a construction home loan product where the service capacity for the principal amount and interest was assessed using an incorrect time period.



731,000

**CUSTOMERS WERE AFFECTED BY
BREACHES**

Up from 568,000 in 2020-21.

4

**BREACHES REQUIRED URGENT MANAGEMENT ATTENTION
AND POSED A SERIOUS RISK TO BUSINESS OPERATIONS**



THE MOST COMMON CAUSE OF BREACHES

50%

**PROCESSES &
PROCEDURES NOT
FOLLOWED**

Up from 45% in 2020-21.

24%

MANUAL ERROR

Down from 35% in 2020-21.

These main causes reflect staff training as the most common remediation action.

SUBSCRIBERS NEED TO IMPROVE RECORD KEEPING

43%

**OF BREACHES DID NOT INCLUDE SPECIFIC DETAILS
FOR LONG-TERM REMEDIATION ACTIVITIES**



Down from 63% in 2020-21.



**REPORTED COMPLAINTS INCREASED
BY 24% TO 36,689**

Key Insights

Quality of reporting needs improvement

Too many Code subscribers reported no breaches or a low number of breaches.

Ten subscribers have reported no breaches for three consecutive reporting periods. Three subscribers with more than \$2 billion in assets have reported less than the industry average mean for five consecutive reporting periods.

The quality of reported breaches in each of the six categories of subscribers varies greatly.

We consider zero breaches to be highly unlikely as we know that mistakes happen. When subscribers continue to tell us they have no breaches, we question the adequacy and effectiveness of their monitoring and reporting systems and capabilities.

Many subscribers have systems and processes to identify, record and report breaches of the Code, and they are investing in improvements. We commend this commitment to a culture of compliance and continuous improvement.

Identifying, recording and reporting Code breaches is not only critical to effectively remediate customers but also to identify systemic issues where improvements can be made. And the improvements deliver better outcomes for customers – an end point that serves everyone, including the bank, well.

However, some subscribers reported inadequate or no breach recording systems. This is unacceptable and must be addressed as a priority.

This will be a strong focus for the Committee in the period ahead and we look forward to seeing the results of the improvements in the next reporting period.

Categorising breaches for meaningful insights

Subscribers must accurately categorise breaches according to specific Code provisions.

This ensures quality data and insights which help pinpoint accountabilities – who the key stakeholders are and how they should be involved in remediation.

Lack of addressing detailed Code provisions

Subscribers reported one third (35%) of breaches under the Key Promises of the 2018 Code, including to provide higher customer service and standards (Key Promise 5) and compliance with legal and industry obligations (Key Promise 8).

Classifying breaches broadly under Key Promises does not provide sufficient information about the nature of the breach and should be a last resort.

Rather than reporting breaches against Key Promises, subscribers should use specific Code obligations wherever possible. This can highlight areas of concern and provide more meaningful information and data.

Key Promises underpin the Code as a set of guiding principles. These promises support the specific obligations set out in the main part of the Code.

By thoroughly understanding breaches and recording them accurately against specific Code obligations, subscribers can improve risk and compliance frameworks and create a positive and proactive compliance culture.

Accurate breach data is a key indicator that a compliance program and its supporting reporting systems are working.

Lack of details about remedial action

For just under half of all breaches, subscribers used the category 'other' to provide details for immediate remedial action. And about three-quarters of breaches did not specify long-term remedial action.

Such reporting practices do not provide sufficient information for the Committee to have confidence that appropriate remediation has been provided.

Many subscribers that did not undertake long-term remediation reported that they assessed the breaches to be 'individual' and not systemic.

Short-term remediation, taken within 48 hours of an incident, was reported for about one third of breaches. Long-term remediation, within one month of an incident, occurred for about one quarter of breaches.

This indicates that subscribers still treat breaches in the same way as complaints. The common approach is to provide a quick fix to each incident when it occurs rather than making the effort to identify and address the root causes of breaches.

An effective review of a failed process or procedure, with the resulting changes and improvements, provides long-lasting improvements.

Subscribers that provide details about long-term remediation can identify and highlight key lessons from each breach. A subscriber with a strong culture of compliance understands the root causes of a breach and a complaint and applies remediation, both short-term and long-term, in response.

Lack of assessment regarding severity and impact

One third of subscribers did not provide details about the severity and management of reported breaches.

Subscribers identified that 228 (9%) breaches were reported to regulators, but only four breaches were identified as a serious risk to business operations requiring urgent management attention.

Assessing the severity and impact of a breach is of vital importance to the business and should be part of its general risk framework.

Some data from subscribers was contradictory. We found subscribers that reported paying compensation to customers affected by a breach but did not report any financial impact from its breaches.

Breach details should include the impact of a breach, including how many customers were affected and the financial impact. This should be determined before remediation or compensation.

Subscribers should also capture details that indicate a breach was identified as systemic and referred to regulators. This should guide assessment of the severity of a breach.

Facing challenges

Transition to the 2022 Code and ongoing regulatory change presented a challenge for many subscribers.

The commencement of ASIC's [Regulatory Guidance 271 – Internal Dispute Resolution](#) on 5 October 2021 meant subscribers had to comply with new requirements for internal dispute resolution and recording and reporting complaints.

We aligned our categories for products involved in breaches with the [ASIC's IDR Data Reporting Handbook](#) to assist subscribers with the collation of data and avoid the duplication of systems.

Product [design and distribution obligations](#) also came into force on 5 October 2021. These obligations require subscribers to design financial products to meet the needs of consumers and to distribute their products in a more targeted manner. This added to compliance frameworks.

There are more regulatory changes coming over the next 12 months and we expect subscribers to fully implement the 2022 Code, with a particular focus on new obligations for small business lending and dealing with customers experiencing vulnerability.

Increase in reported complaints

In 2021-22, we saw a significant increase in the number of complaints reported by subscribers.

The number of complaints rose from 29,650 in 2020-21 to 36,689 in 2021-22: an increase of 24%.

We heard from subscribers about an increased awareness of issues among customers since the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in 2019. Reportedly, this has led to more questions for financial institutions from customers when engaging in services.

Consequently, subscribers are hearing more from customers and dealing with more requests, concerns and correspondence.

Also contributing to the rise in complaints was aligning our categories for product, issue, outcome and timeframe with [ASIC's IDR Data Reporting Handbook](#). These changes were designed to make it easier for subscribers to update their reporting systems to reflect ASIC's IDR categories and provide information about complaints for their ACS.

The increased awareness from customers about issues with financial services as well as the improved categories for complaints is likely to have contributed to the increase in complaints numbers.

In 2021-22, due to the alignment with ASIC categories, a comparison with complaints categories of previous years is not possible. See Part C of this report for a full breakdown of complaints data.

Subscribers should use complaints data to improve products and services.

We expect to see subscribers thoroughly examine the nature and root causes of the complaints they report to identify ways they can rectify issues and prevent reoccurrence.

Investing in technology and reporting capabilities to analyse complaints data is important.

This will help identify areas for improvement in the complaints process and in products and services.

Enhanced diagnostic capabilities as well as a culture that values complaints, will produce beneficial outcomes for both customers and customer owned banking institutions.

Looking ahead

The new 2022 Code provides an opportunity for widespread improvements.

Following the challenges of 2021-22 and seeing the efforts from subscribers to overcome them, we expect significant improvements in reporting breaches and complaints across the industry in 2022-23.

The 2022-23 reporting period will be the first full reporting period for which the 2022 Code applies.

Over the next 12 months we will focus our attention on compliance with the new obligations in the 2022 Code. We look forward to seeing the developments in compliance processes and procedures as the obligations in the 2022 Code take effect.

All subscribers must have a strong compliance framework to meet their obligations. This is the backbone of a culture of compliance that embraces monitoring and reporting as part of a pursuit of better outcomes for customers.

Busting misconceptions

WE HAVE IDENTIFIED SOME COMMON MISCONCEPTIONS THAT WE BELIEVE ARE CONTRIBUTING TO UNDER REPORTING OR NON-REPORTING OF CODE BREACHES. BELOW WE CLARIFY THE EXPECTATION AND PROVIDE SOME TIPS TO IMPROVE PRACTICE.

MISCONCEPTION:

'If there are no consumer complaints, then there are no Code breaches.'

REALITY: Customer complaints and breaches are not always linked. Sometimes a customer complaint does not constitute a breach, and sometimes breaches do not stem from a complaint.

TIP: Make sure all staff know exactly what constitutes a breach and have separate registers for breaches and customer complaints.

MISCONCEPTION:

'If we resolve a failure to the customer's satisfaction without any detriment, then it is not a breach.'

REALITY: Failing to provide a service in accordance with the obligations of the Code is a breach regardless of the outcome of any remediation.

TIP: Record and report all incidents that might constitute a Code breach. This helps to identify systemic issues that can be addressed to improve practice.

MISCONCEPTION:

'Key Promises is the main part of the Code and we should categorise breaches against it.'

REALITY: Key Promises is a set of guiding principles, but it is not the main part against which a subscriber records all breaches.

TIP: Categorise breaches against the primary reason for non-compliance using a specific Code obligation.

MISCONCEPTION:

‘It is good to have no breaches.’

REALITY: Reporting no breaches is not a shortcut to a good reputation. In fact, it suggests inadequate processes and procedures for identifying, recording and remediating breaches.

TIP: Identify, record and report breaches to identify areas for improvement and deliver better outcomes for customers.

MISCONCEPTION:

‘Recording breaches is limited to certain people or teams.’

REALITY: For comprehensive compliance monitoring, all staff should be able to record breaches. Everyone must understand the benefits of accurate record-keeping and be able to record all data.

TIP: Do not limit reporting breaches. Encourage and support staff of all levels and all areas to identify and report any breach.

MISCONCEPTION:

‘A breach has no financial impact if we compensated the customer or took remedial action.’

REALITY: The compensation or remedial action determines the financial impact of a breach.

TIP: Calculate and record the financial impact regardless of the subsequent compensation or remedial action.

MISCONCEPTION:

‘The complaints register and breach register are the same.’

REALITY: These are conceptionally different and conflating them is a problem because they represent different issues and come from different practices.

TIP: Establish a breach register and a separate complaints register that all staff understand and can use.

Data Analytics

Part A: Details of Code subscribers

Table 1: Number of subscribers by state (head office) and size of operation

Category by assets in 2021-22	NSW	NT	Qld	SA	Tas	Vic	WA	Total	2020-21
Category AA more than \$5b in assets	3	-	2	2	-	1	1	9	8
Category A \$2b to \$5b in assets	2	-	2	-	-	2	-	6	7
Category B \$1b to \$2b in assets	6	-	-	2	1	2	-	11	11
Category C \$500m to \$1b in assets	6	-	2	-	-	1	-	9	8
Category D \$200m to \$500m in assets	7	-	2	-	-	2	-	11	11
Category E up to \$200m in assets	4	1	-	1	-	3	-	9	12
Total 2021-22	28	1	8	5	1	11	1	55	57
Compared to 2020-21	28	1	8	5	1	13	1	57	
Compared to 2019-20	29	1	9	5	1	14	1	60	
Compared to 2018-19	31	1	9	5	1	14	1	62	

Table 2: Number of branches (including head office) by state and size of operation

	ACT	NSW	NT	Qld	SA	Tas	Vic	WA	Total	%	2020-21
Category AA	10	111	5	77	41	-	27	25	296	46%	298
Category A	5	53	3	55	2	1	9	2	130	20%	134
Category B	-	56	1	4	8	7	18	2	96	15%	119
Category C	-	35	-	12	-	-	10	-	57	9%	53
Category D	-	23	-	15	1	-	3	1	43	7%	42
Category E	-	5	14	-	1	-	2	-	22	3%	35
Total 2020-21	15	283	23	163	53	8	69	30	644		681
Total %	2%	44%	4%	25%	8%	1%	11%	5%			
Compared to 2020-21	16	283	23	157	74	8	77	43	681		
Compared to 2019-20	17	318	23	160	54	8	84	34	698		
Compared to 2018-19	18	296	15	181	55	6	39	35	699		

Table 3: Number of members, accounts and staff by size of operation in 2021-22

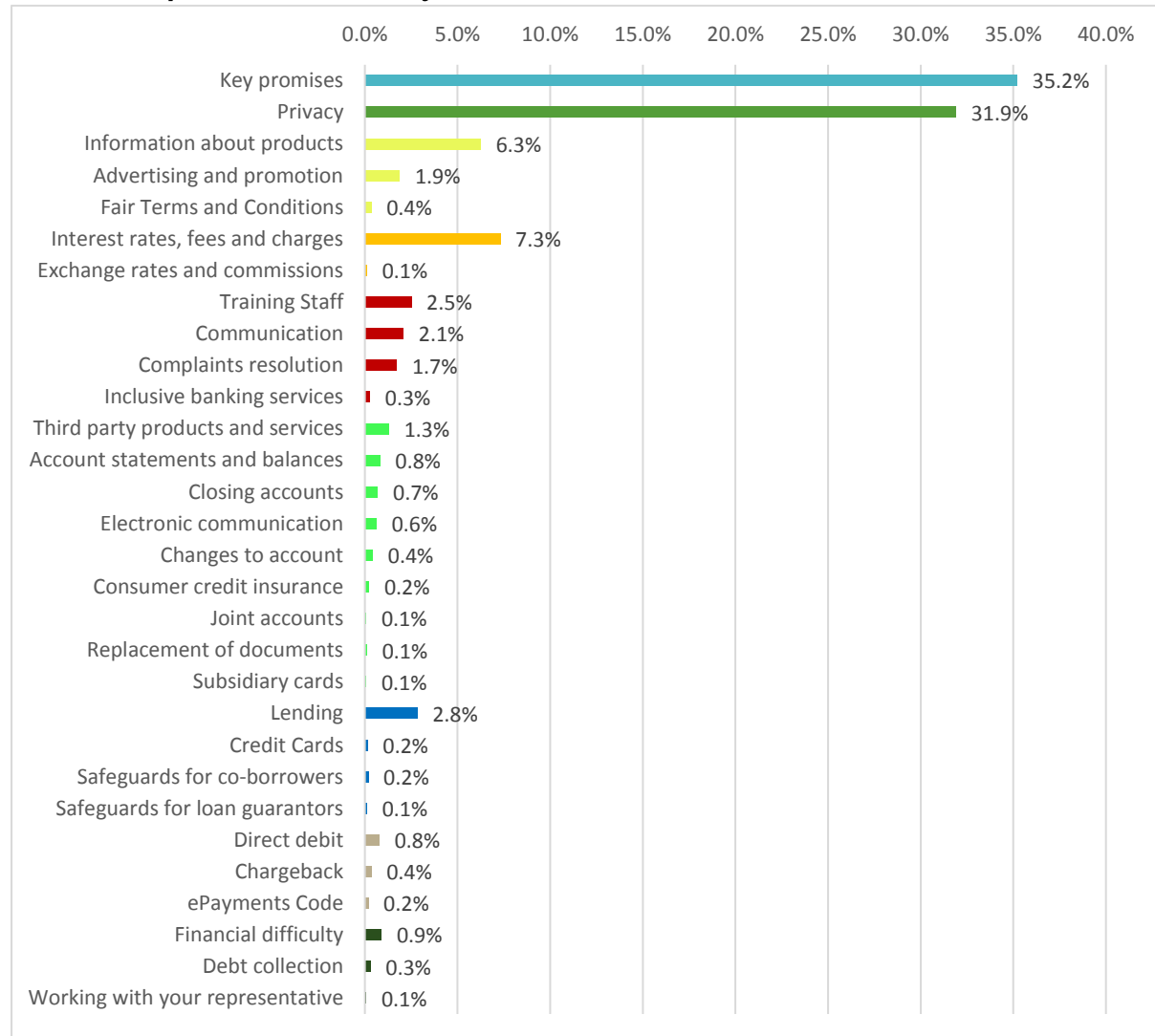
	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Total members	2,287,185	530,005	434,874	186,056	110,637	60,026	3,608,783
Total accounts	5,220,917	2,107,126	1,102,198	371,896	191,444	140,014	9,133,595
Staff numbers							
Up to 20 staff	-	-	-	-	4	8	12
21 to 30 staff	-	-	-	-	2	-	2
31 to 50 staff	-	-	-	-	1	4	5
51 to 100 staff	-	-	4	8	1	1	14
Over 100 staff	9	6	7	-	-	-	22

Part B: Breach data

Note: Because not all subscribers provided conclusive information for each category, data in the tables and charts related to self-reported breaches are indicative only.

B.1 Areas of concern by Code breach nature

Chart 1: Reported breaches by nature in 2021-22



Note: Categories with no breaches in 2021-22 are not included.

Chart legend – Code sections by colour

- Our promises to you
- Our commitment to your privacy and security
- How we inform you about our products
- Our approach to fees, rates, and commissions

- Our customer service standards
- When you have an account with us
- Our approach to lending
- Our approach to payments
- Support for customers experiencing financial difficulty

B.2 Impact of self-reported breaches

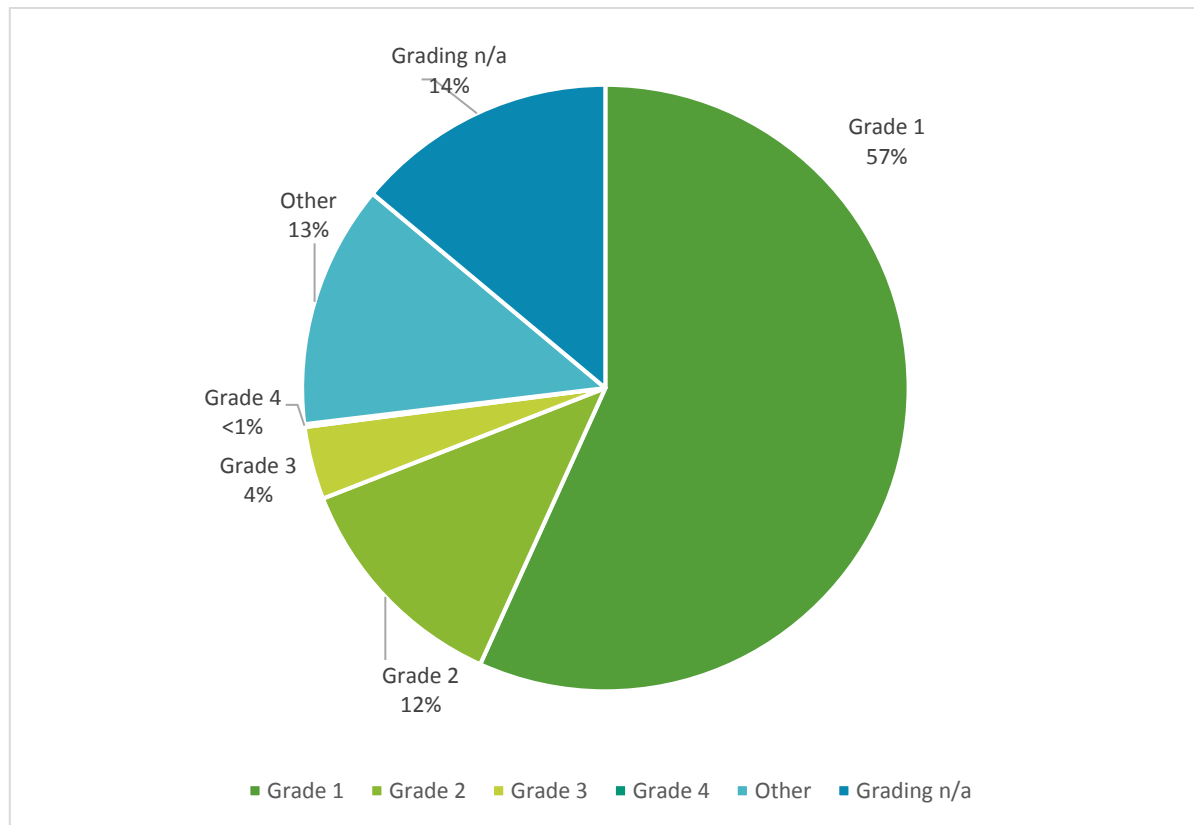
Table 4: Impact of reported breaches by Code obligation in 2021-22

Code obligation	Breaches	Customers impacted	Financial impact
Key promises	894	366,332	\$31,540,231
Privacy	811	23,873	\$729,742
Financial difficulty	23	3,182	\$318,932
Interest rates, fees and charges	186	33,614	\$261,244
Third party products and services	33	250	\$216,359
Closing accounts	18	17,843	\$178,140
Advertising and promotion	48	144,216	\$147,451
Training Staff	64	182	\$67,866
Communication	54	13,837	\$57,510
Lending	72	756	\$41,058
Information about products	159	94,220	\$29,520
Vulnerable customers	7	8	\$18,000
Chargeback	9	9	\$17,550
Direct debit	20	45	\$14,890
Consumer credit insurance	6	6	\$8,824
ePayments Code	5	5	\$6,367
Term deposits	1	6,652	\$5,155
Credit Cards	4	3	\$4,050
Changes to account	11	1,535	\$2,243
Joint accounts	2	2	\$2,171
Replacement of documents	3	53	\$1,594
Exchange rates and commissions	3	3	\$627
Complaints resolution	44	123	\$450
Working with your representative	2	2	\$285
Account statements and balances	21	17,782	\$17
Subsidiary cards	2	2	\$0
Safeguards for loan guarantors	3	16	\$0
Fair Terms and Conditions	9	4,104	\$0
Safeguards for co-borrowers	5	6	\$0
Reverse mortgage loans	1	700	\$0
Electronic communication	16	1,463	\$0
Debt collection	8	90	\$0
Total	2,544	730,914	\$33,670,276

Table 5: Impact of reported breaches by product or service type in 2021-22

Code obligation	Breaches	Customers impacted	Financial impact
Consumer Credit (ASIC reference 9 to 22)	857	262,303	\$30,329,541
Financial advice or credit assistance (ASIC reference 185 to 187)	20	704	\$1,190,712
Not product/service related (ASIC reference 188)	243	53,701	\$562,531
Savings accounts (ASIC reference 34 to 39)	298	115,429	\$344,210
Current accounts (ASIC reference 27 to 32)	441	102,322	\$227,887
Direct transfer (ASIC reference 126 to 136)	137	1,248	\$165,092
Business Finance (ASIC reference 1 to 8)	7	140	\$40,281
Non-cash (ASIC reference 137 to 142)	32	16	\$165
Guarantees (ASIC reference 23 to 25)	2	16	\$0
Securities (ASIC reference 106 to 113)	2	1	\$0
Traditional trustee services (ASIC reference 179 to 184)	1	3	\$0
Real property (ASIC reference 105)	1	2	\$0
Managed investments (ASIC reference 88 to 104)	1	1	\$0
Other (not classified with ASIC reference)	502	195,028	\$809,857
Total	2,544	730,914	\$33,670,276

Chart 2: Grading of reported breaches in 2021-22



Description of the Grades	
Grade 1	An action or incident that requires management attention but does not impose a serious risk to business operations or the Australian Financial Services (AFS) licence.
Grade 2	An action or incident that requires immediate management attention. It can be an accumulation of three Grade 1 actions or incidents.
Grade 3	An action or incident that poses a significant risk to business operations or the AFS licence or has resulted in direct financial loss by a customer. It can be one action or incident or an accumulation of four or more Grade 1 or two or more Grade 2 actions or incidents.
Grade 4	An action or incident that requires urgent management attention and poses a serious risk to business operations or the AFS licence (includes major compliance failures, training inadequacies and overall poor performance).
Grade 5	An action or incident that poses a catastrophic risk to business operations or the AFS licence and cannot be rectified.

Table 6: Number of systemic-reported breaches per Code obligation in 2021-22

Code obligation	Cat AA	Cat A	Cat B	Cat C	Cat D	Total
Key promises	46	1	9	6	-	62
Privacy	6	11	-	7	-	24
Interest rates, fees and charges	1	9	-	-	2	12
Information about products	5	-	-	1	-	6
Electronic communication	2	-	-	-	-	2
Account statements and balances	2	-	-	-	-	2
Complaints resolution	2	-	-	-	-	2
Debt collection	-	-	1	-	-	1
Safeguards for loan guarantors	1	-	-	-	-	1
Changes to account	-	-	1	-	-	1
ePayments Code		-	-	1	-	1
Advertising and promotion	1	-	-	-	-	1
Third party products and services	1	-	-	-	-	1
Closing accounts	-	1	-	-	-	1
Total	67	22	11	15	2	117

Note: Category E subscribers did not self-report any systemic breaches.

B.3 Identification of self-reported breaches

Table 7: Identification of reported breaches by subscriber category in 2021-22

<i>Identification method</i>	<i>Cat AA</i>	<i>Cat A</i>	<i>Cat B</i>	<i>Cat C</i>	<i>Cat D</i>	<i>Cat E</i>	<i>Total</i>
Internal process or report	45.8%	30.4%	13.9%	10.9%	5.9%	0.0%	32.9%
Client query or complaint	29.7%	12.9%	59.2%	38.3%	64.7%	73.7%	30.2%
Staff self-identification	8.9%	24.0%	19.9%	27.7%	17.6%	15.8%	16.8%
Random internal audit	7.4%	25.0%	1.7%	15.2%	0.0%	5.3%	12.5%
External compliance audit	0.9%	0.4%	0.3%	0.4%	0.0%	0.0%	0.6%
Other	7.2%	7.3%	4.9%	7.4%	11.8%	5.3%	7.0%

Table 8: Root cause of reported breaches by subscriber category in 2021-22

<i>Root cause</i>	<i>Cat AA</i>	<i>Cat A</i>	<i>Cat B</i>	<i>Cat C</i>	<i>Cat D</i>	<i>Cat E</i>	<i>Total</i>
Process & procedure not followed	49.4%	65.8%	21.4%	45.7%	29.4%	5.3%	49.6%
Manual error	27.8%	13.6%	22.8%	32.8%	29.4%	78.9%	23.9%
System error or failure	6.1%	5.2%	17.9%	8.2%	17.6%	0.0%	7.7%
Incorrect process & procedure	5.9%	9.3%	9.2%	2.7%	0.0%	5.3%	7.0%
Insufficient training	1.2%	5.0%	6.1%	3.5%	5.9%	0.0%	3.2%
Mail house error	0.2%	0.1%	0.9%	5.1%	5.9%	0.0%	0.8%
Staffing/resourcing issues	0.1%	0.1%	4.6%	0.4%	0.0%	5.3%	0.8%
Staff misconduct	0.2%	0.0%	0.3%	0.0%	0.0%	0.0%	0.1%
Other	9.1%	0.8%	16.8%	1.6%	11.8%	5.3%	7.0%

B.4 Remediation of self-reported breaches

Table 9: Actions and timelines for short-term remediation in 2021-22

Actions	Time frame									Total
	Immediate	Within 48 hours	Within 1 week	Within 2 weeks	Within 1 month	1 to 3 months	3 to 6 months	6 to 12 months	Other	
Training	37	52	53	36	151	99	55	7	87	577
Apology	152	83	85	40	58	10	3	3	7	441
Refund of fees/charges	17	8	31	11	16	18	2	1	1	105
Ex-gratia payment	18	13	18	6	15	7	2	-	-	79
Review of and changes to procedure	9	2	5	3	4	5	19	1	4	52
Review of and changes to process	5	7	4	3	11	3	3	-	2	38
Undertaking	2	3	14	3	6	2	2	2	2	36
Premium adjustment	4	2	2	-	4	1	1	-	-	14
Refund of premium	-	4	1	-	4	1	3	-	-	13
Review of and changes to terms and conditions	-	-	-	-	-	2	-	1	1	4
Other	276	148	245	88	153	86	36	13	140	1,185

Table 10: Actions and timelines for long-term remediation in 2021-22

Actions	Time frame						Total
	Within 1 month	1 to 3 months	3 to 6 months	6 to 12 months	1 to 2 years	2 to 5 years	
Training	423	79	17	4	-	-	523
Review of and changes to process	37	19	20	7	4	-	87
Review of and changes to procedure	35	19	8	12	9	-	83
Apology	37	2	3	-	1	-	43
Ex-gratia payment	7	-	-	1	-	-	8
Refund of fees/charges	4	1	1	-	-	-	6
Premium adjustment	3	-	-	-	-	-	3
Review of and changes to terms and conditions	-	2	1	-	-	-	3
Undertaking	2	-	-	-	-	-	2
Refund of premium	-	-	-	1	-	-	1
Other	108	19	14	13	13	1	168

Part C: Complaints data

C.1 Complaints by categories

Chart 3: Top product categories of reported complaints in 2021-22 (minimum 1%)

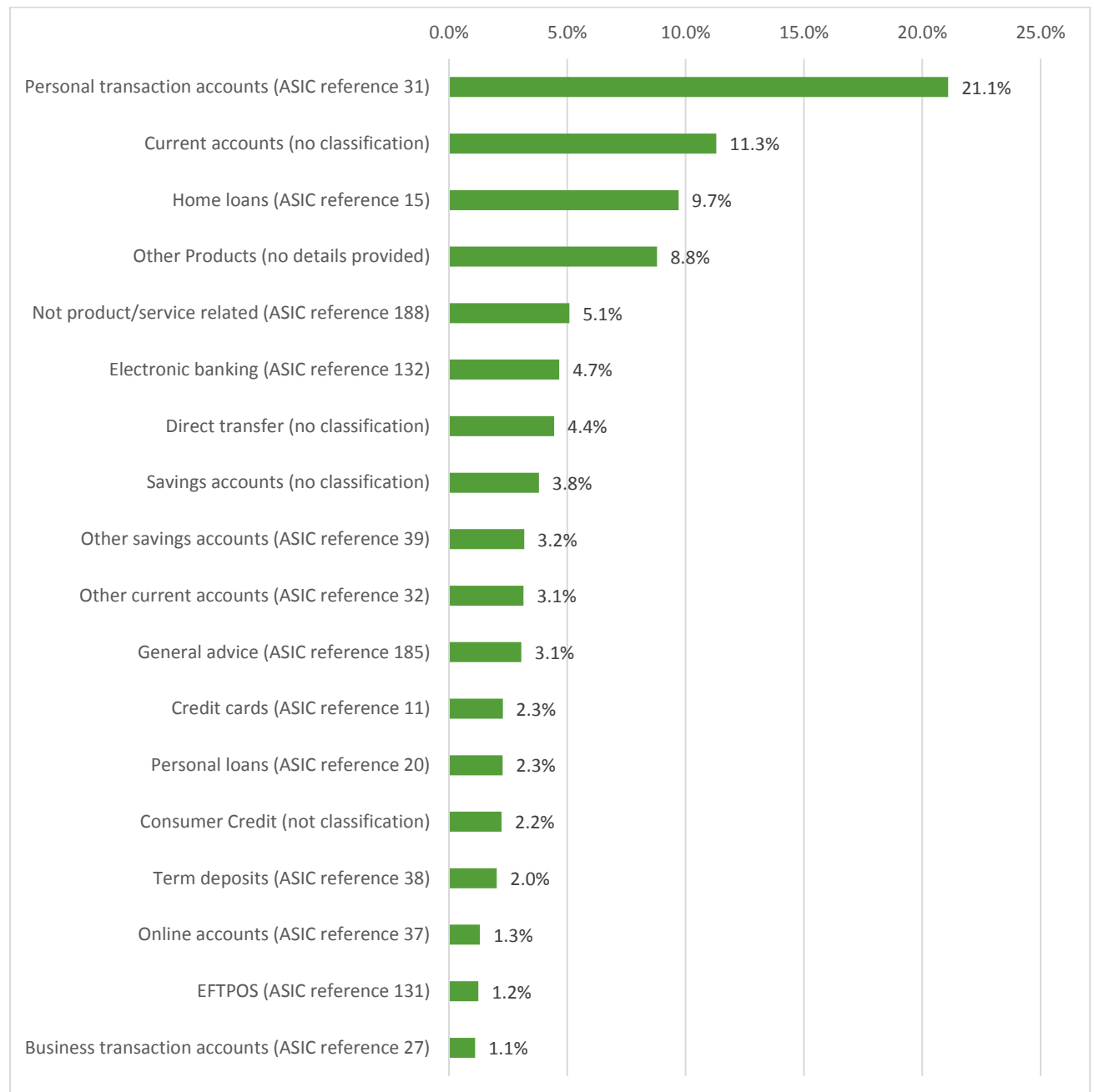


Chart 4: Top categories of reported complaints in 2021-22 (minimum 1%)

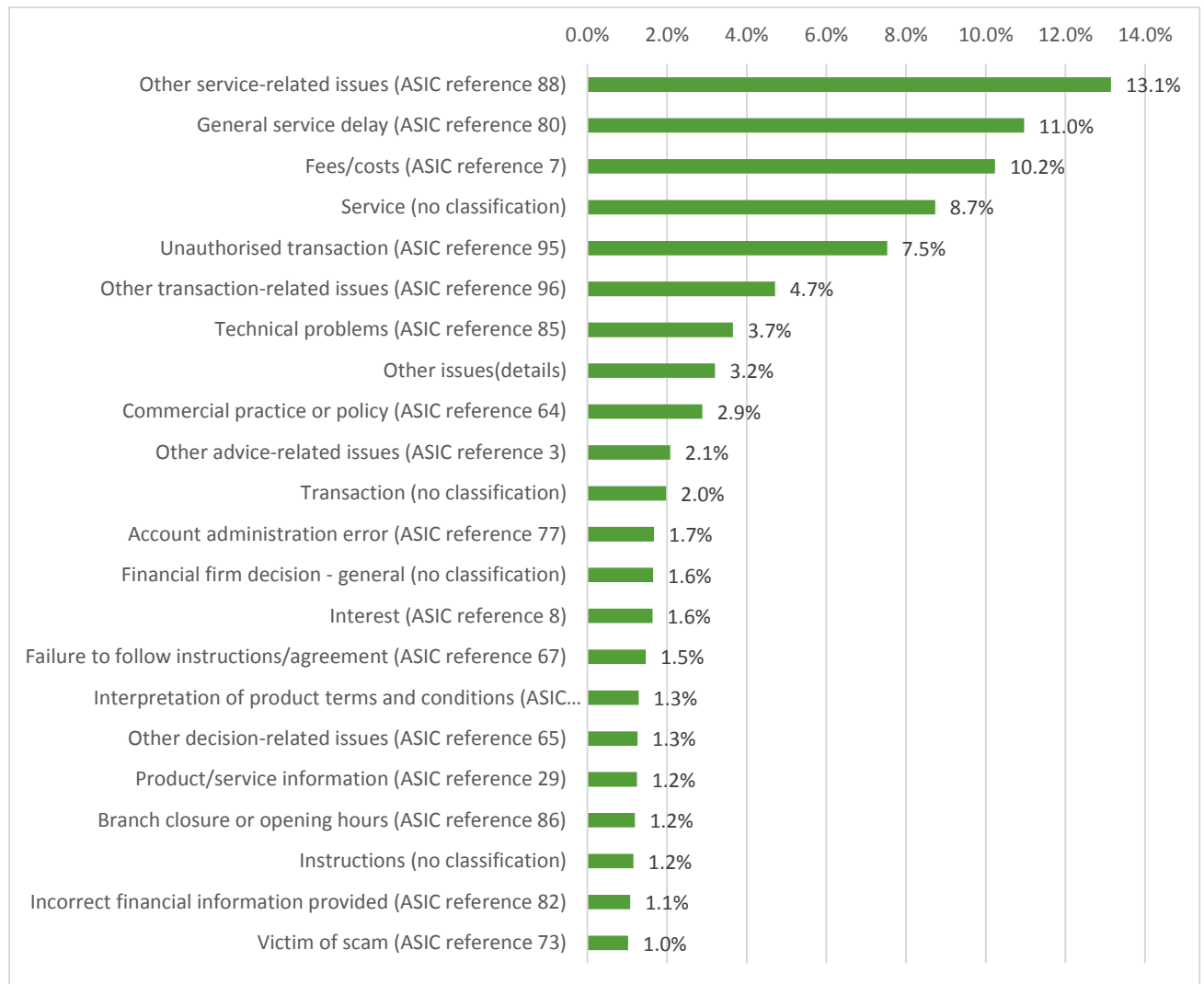
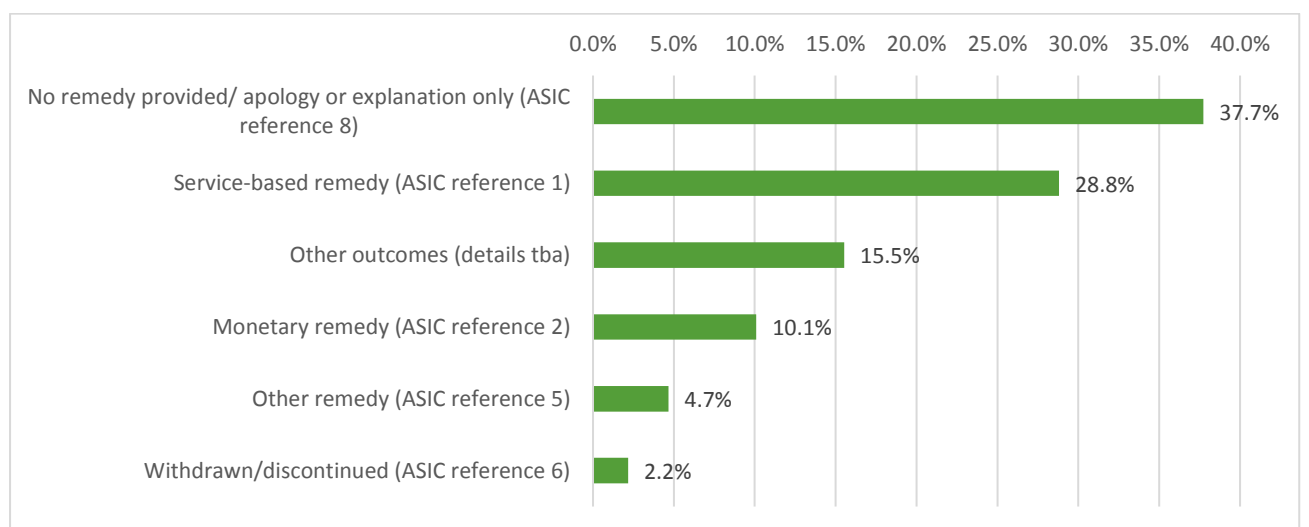


Chart 5: Top outcomes of reported complaints in 2021-22 (minimum 1%)



Part D. Data trends

Chart 6: Trends and relationships in breach and complaints data

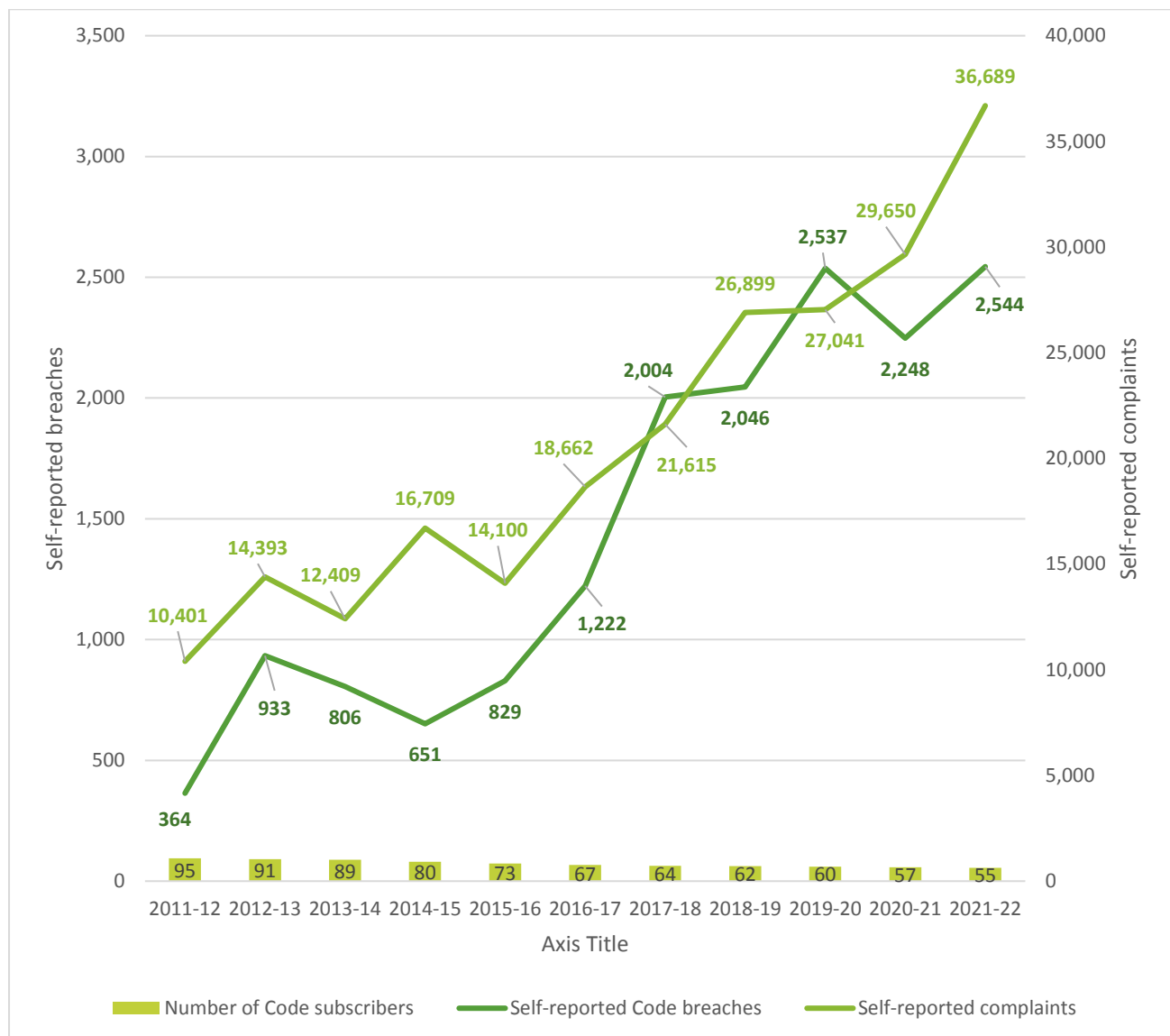
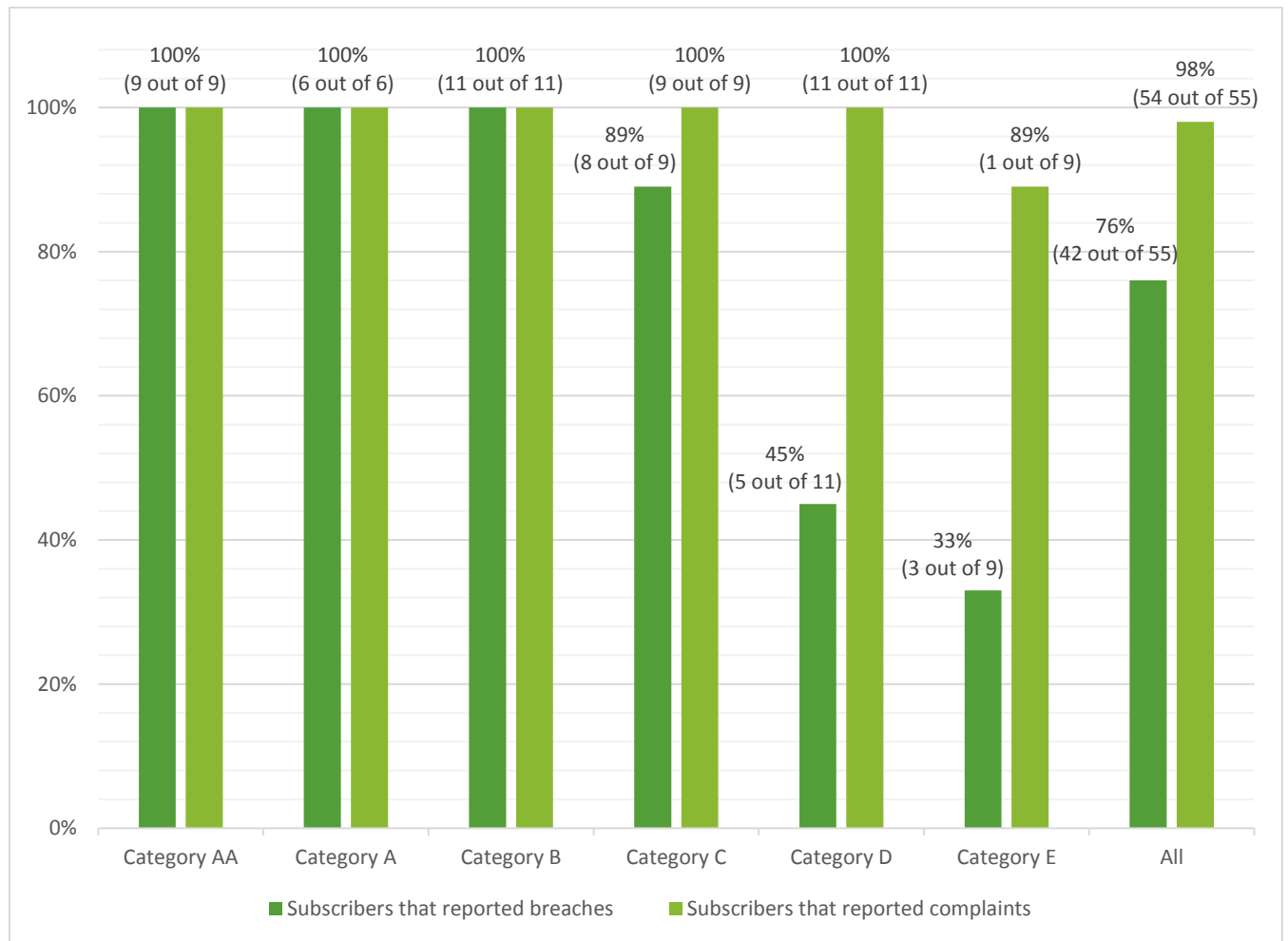


Chart 7: Reporting culture in 2021-22



Part E. Breach data of the past five years

Charts 8 to 14 compare the self-reported Code breaches per category of subscriber according to business size. Charts include 'industry' and 'sector' mean figures:

- The 'industry' figure is calculated using the total number of self-reported breaches by the total number of subscribers. This indicates the overall industry performance.
- The 'sector' figure is calculated using the total number of self-reported breaches by the total number of subscribers within that size of business. This provides a benchmark for comparison.

Chart 8: Self-reported breaches per subscriber in Category AA

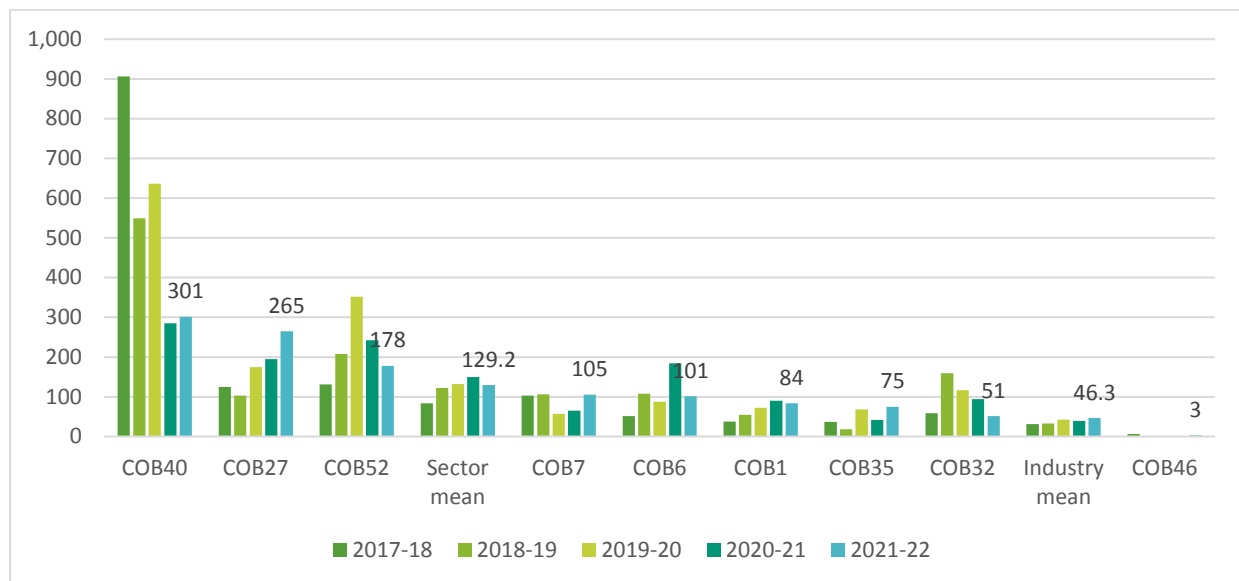


Chart 9: Self-reported breaches per subscriber in Category A

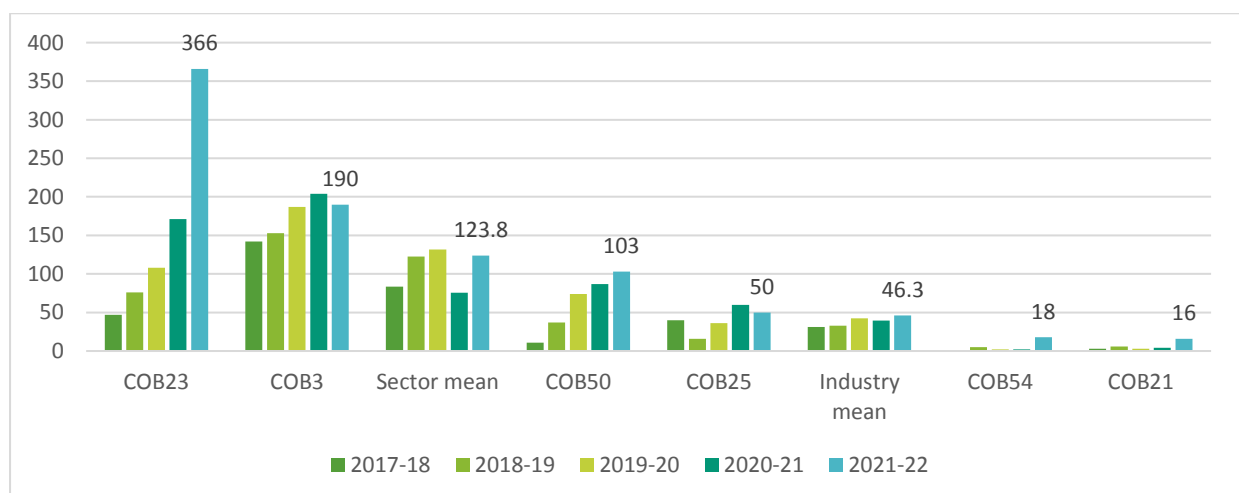


Chart 10: Self-reported breaches per subscriber in Category B

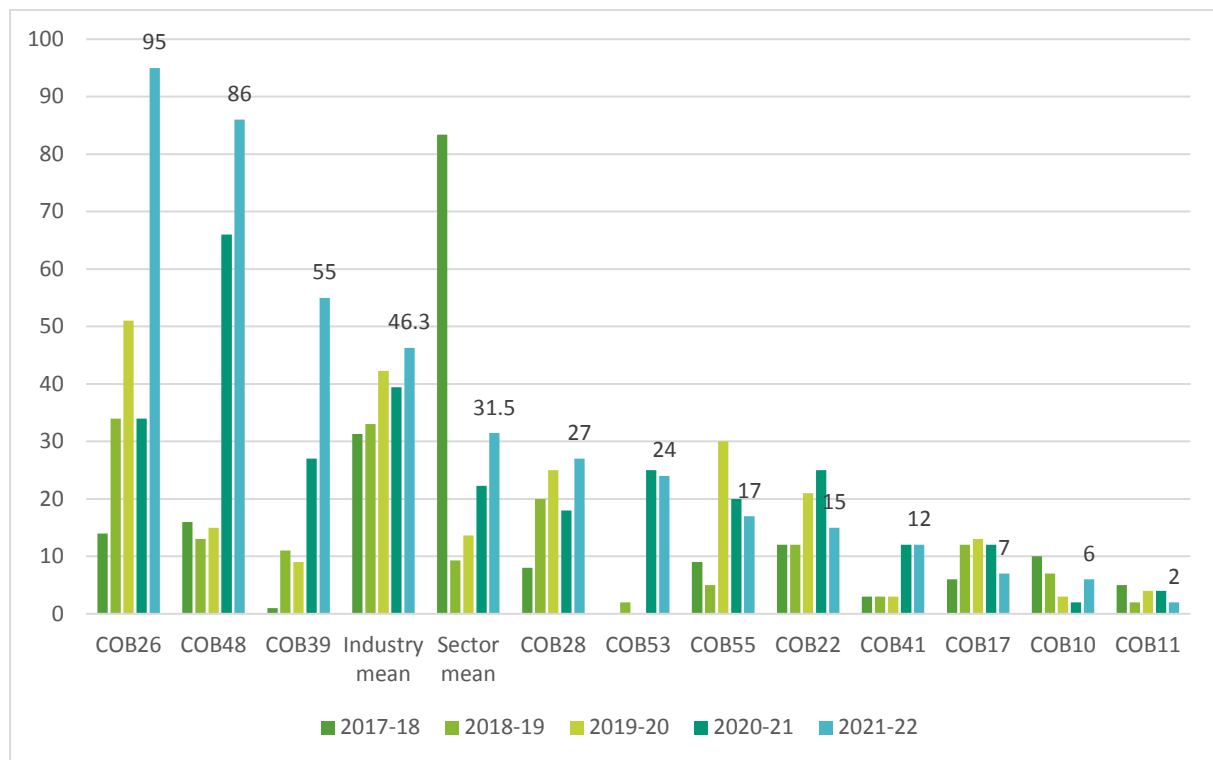


Chart 11: Self-reported breaches per subscriber in Category C

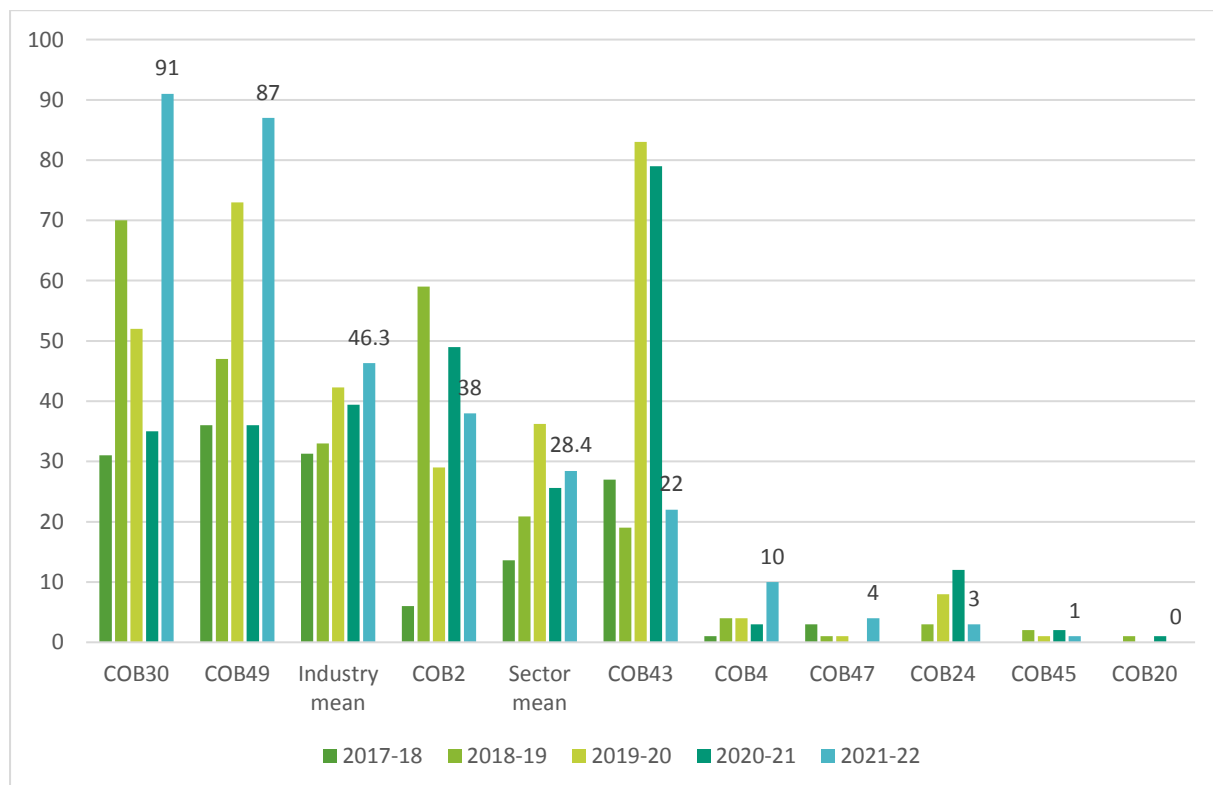


Chart 12: Self-reported breaches per subscriber in Category D

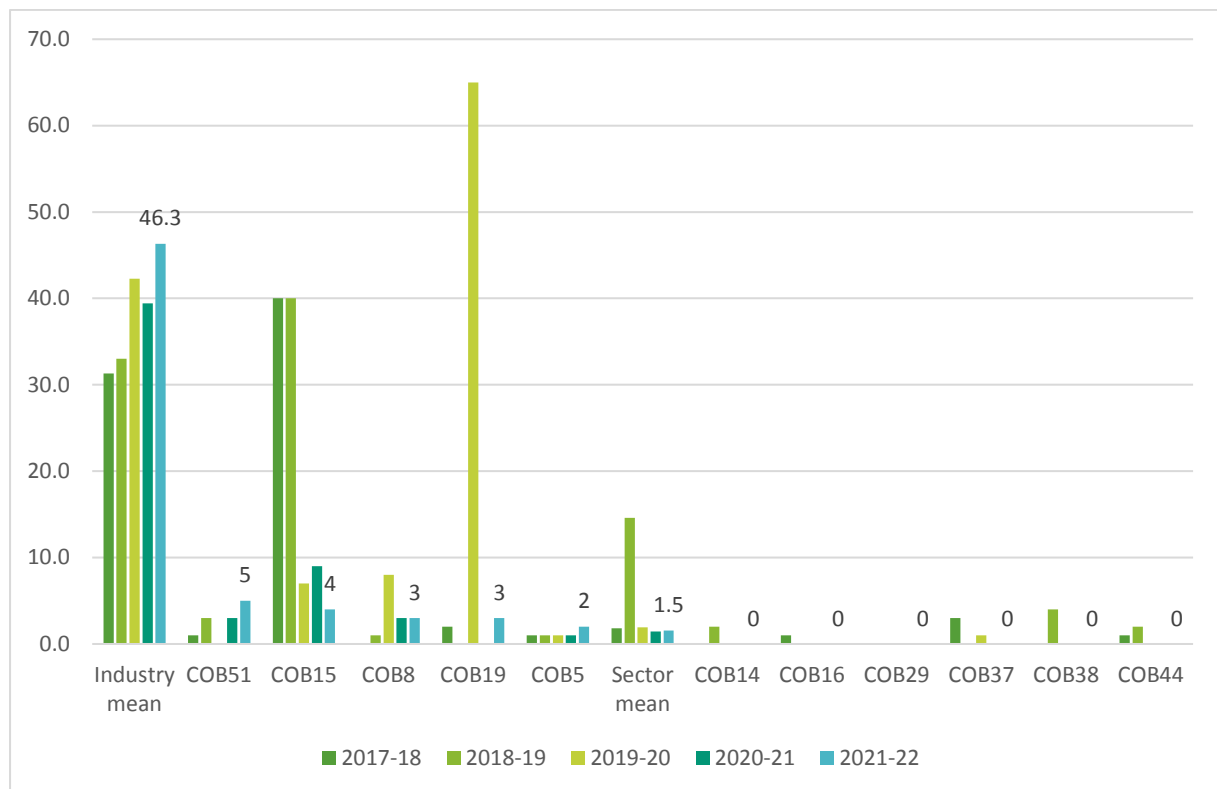


Chart 13: Self-reported breaches per subscriber in Category E

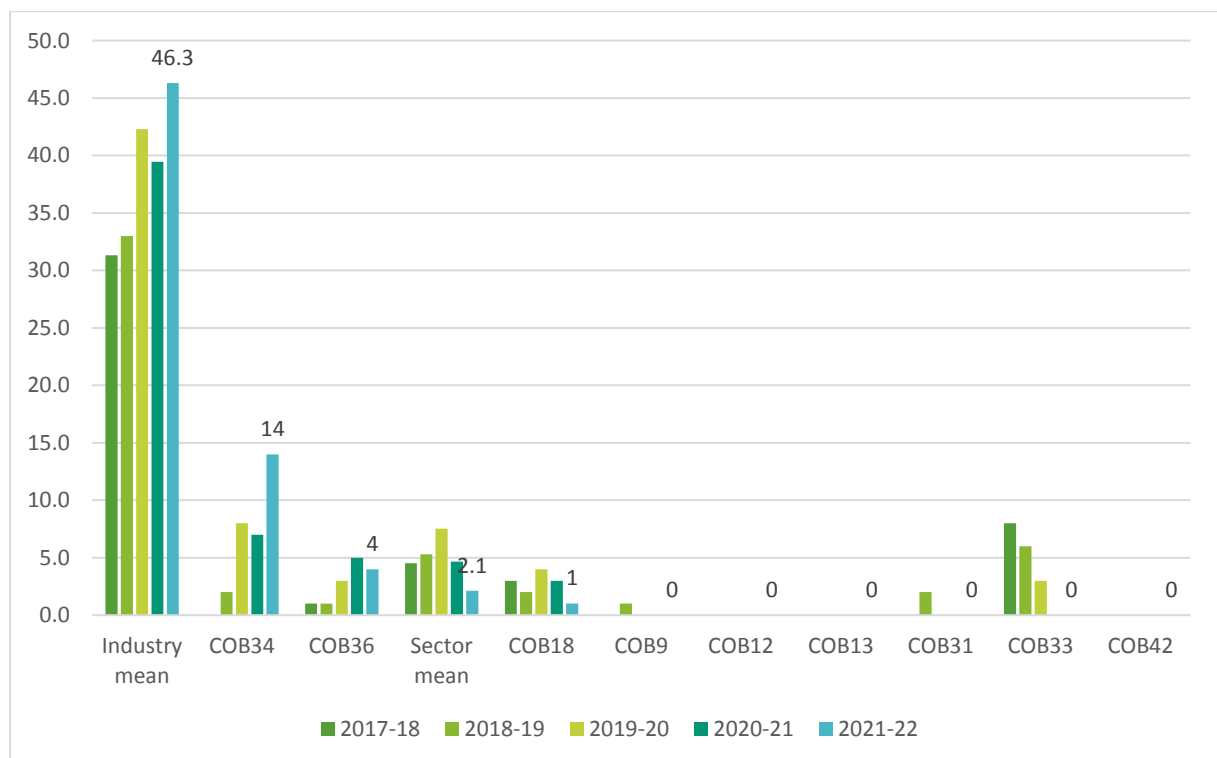
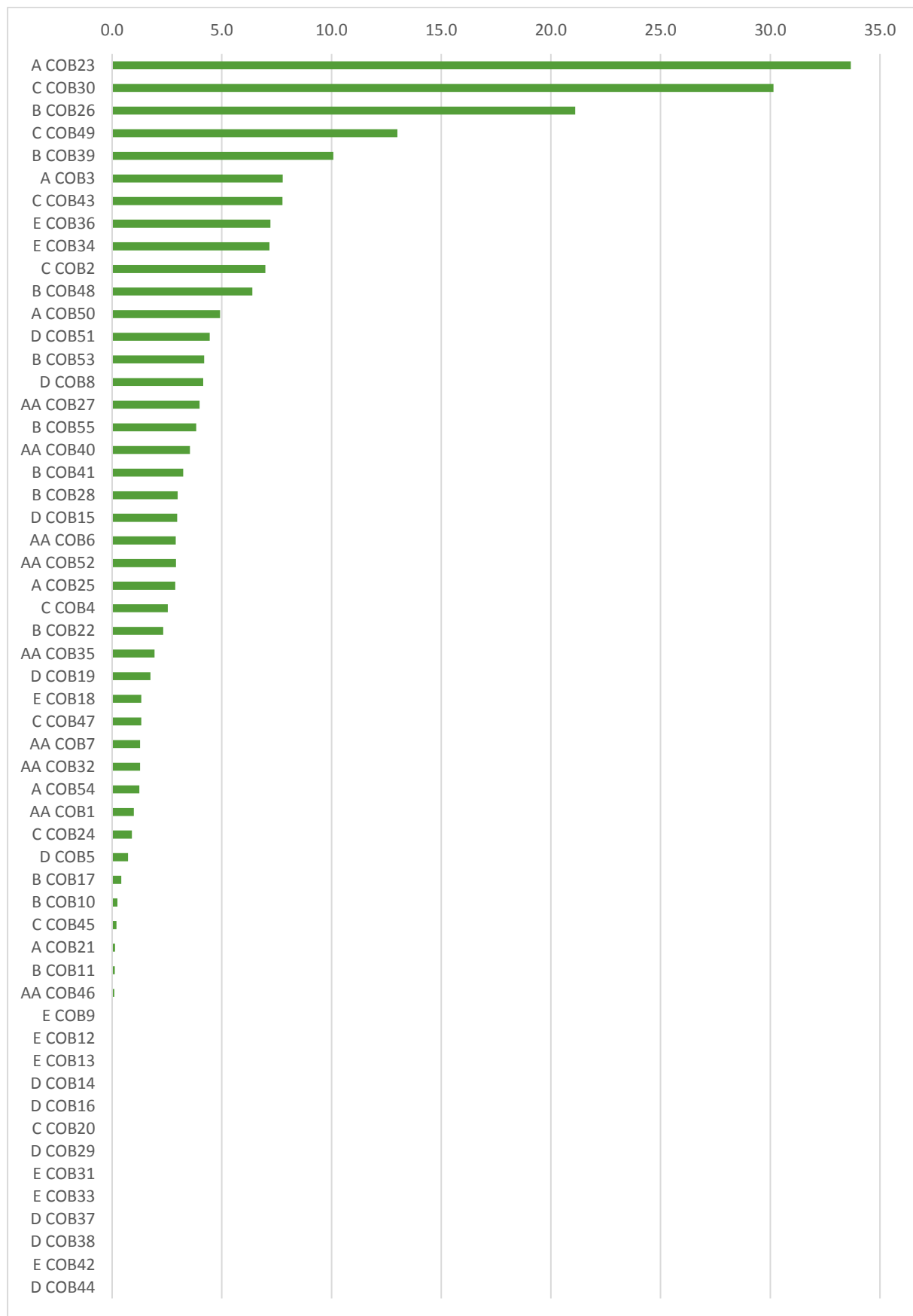


Chart 14: Self-reported breaches per 10,000 accounts in 2021-22



Part F. Complaints data of the past five years

Charts 15 to 21 compare the number of self-reported complaints per category of subscriber according to business size. Charts include 'industry' and 'sector' mean figures:

- The 'industry' figure is calculated using the total number of self-reported complaints by the total number of subscribers. This indicates the overall industry performance.
- The 'sector' figure is calculated using the total number of self-reported complaints by the total number of subscribers within that size of business. This provides a benchmark for comparison.

Chart 15: Self-reported complaints per subscriber in Cat AA

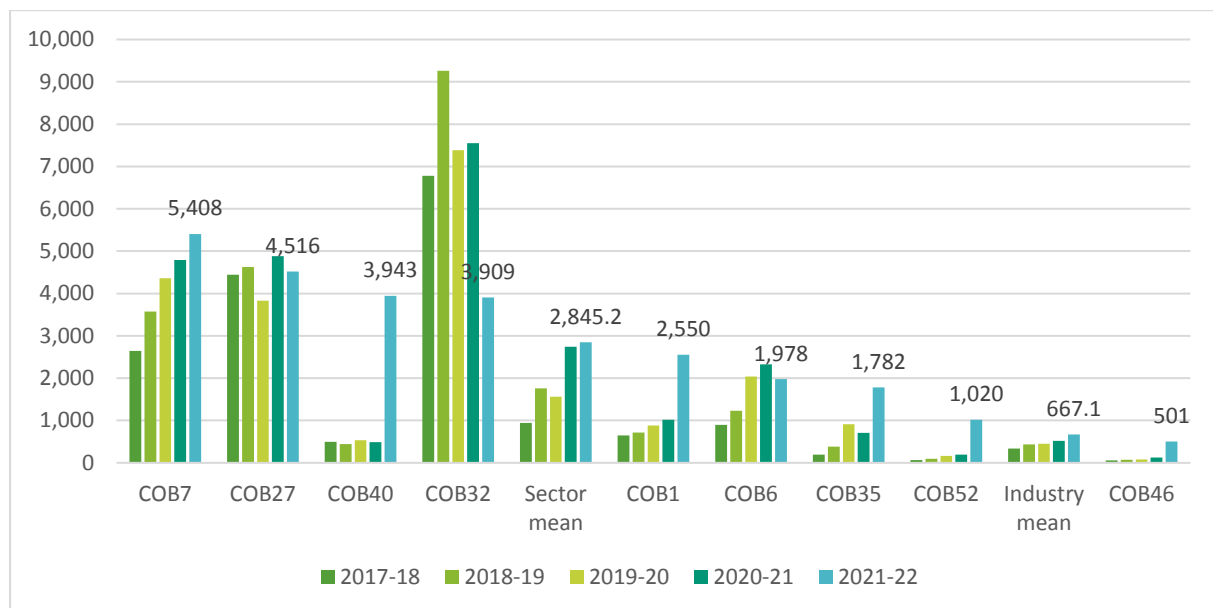


Chart 16: Self-reported complaints per subscriber in Cat A

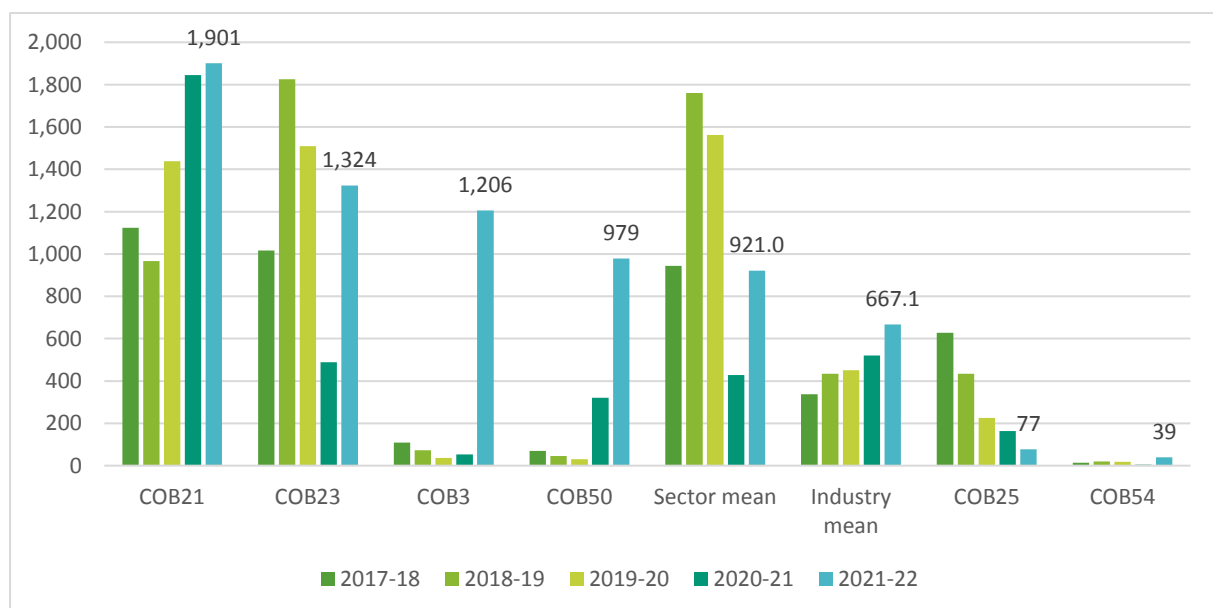


Chart 17: Self-reported complaints per subscriber in Category B

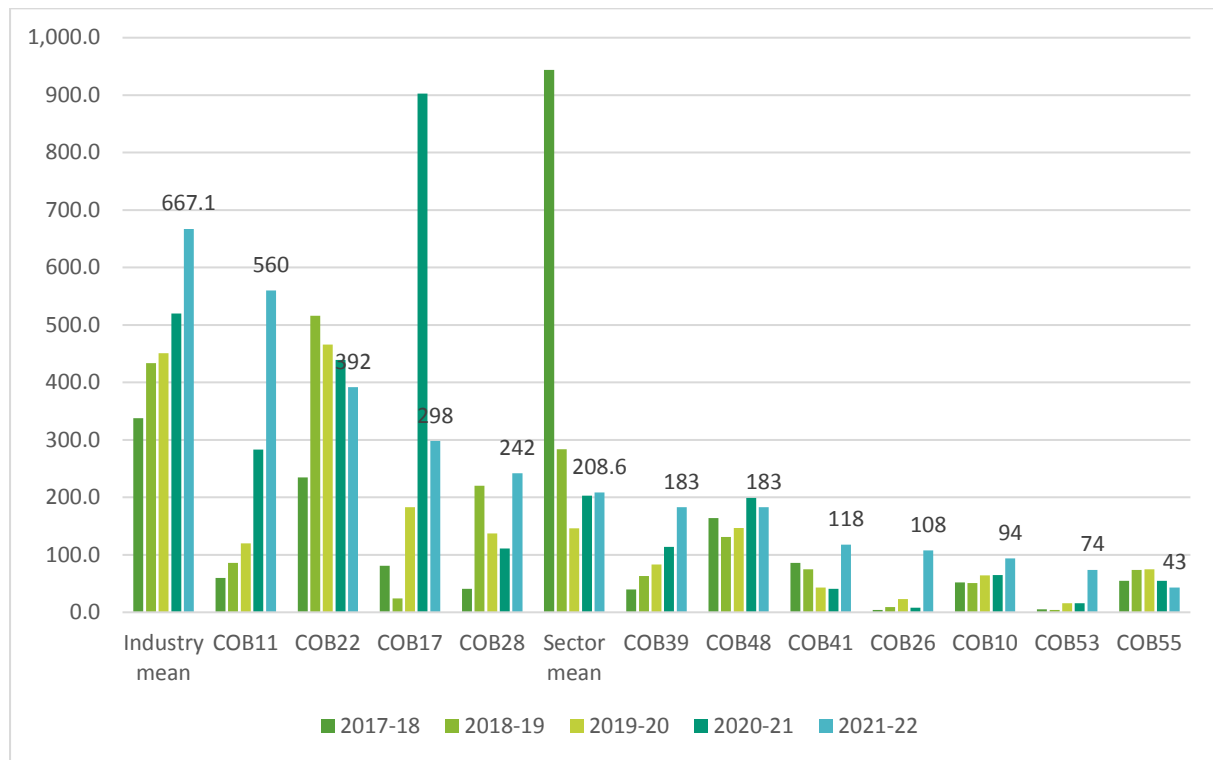


Chart 18: Self-reported complaints per subscriber in Category C

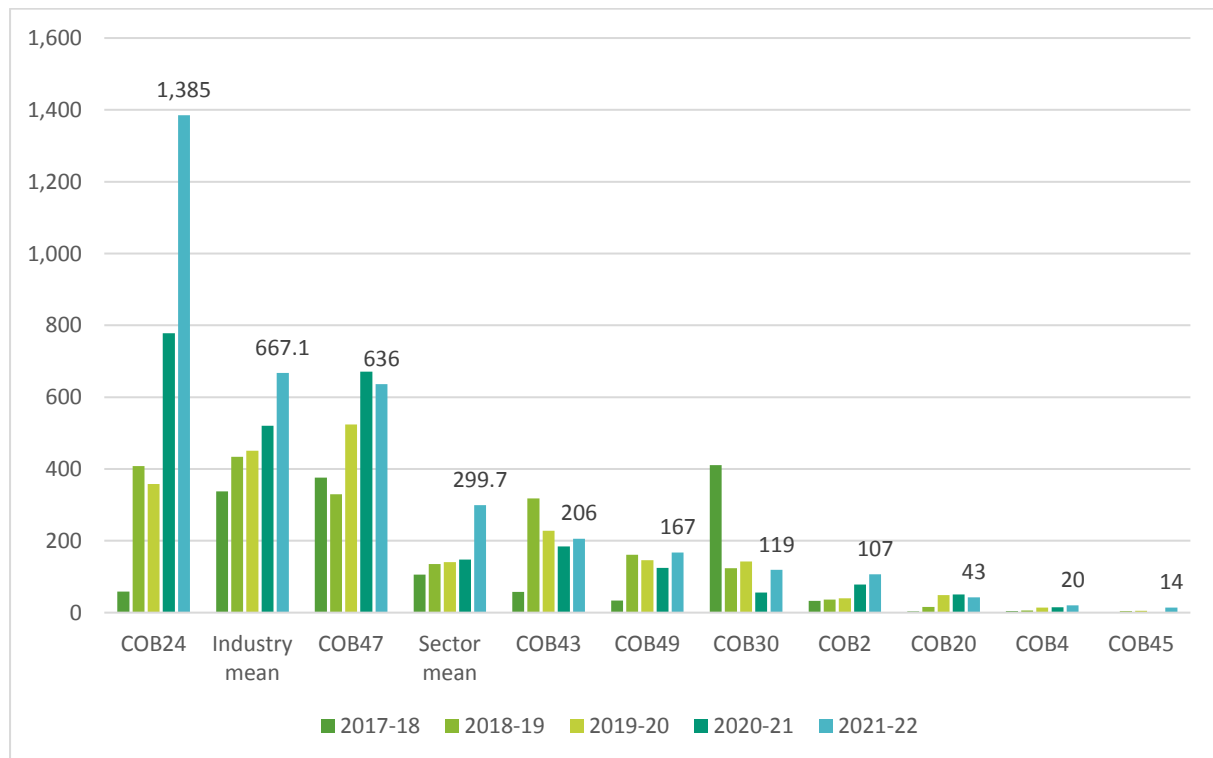


Chart 19: Self-reported complaints per subscriber in Category D

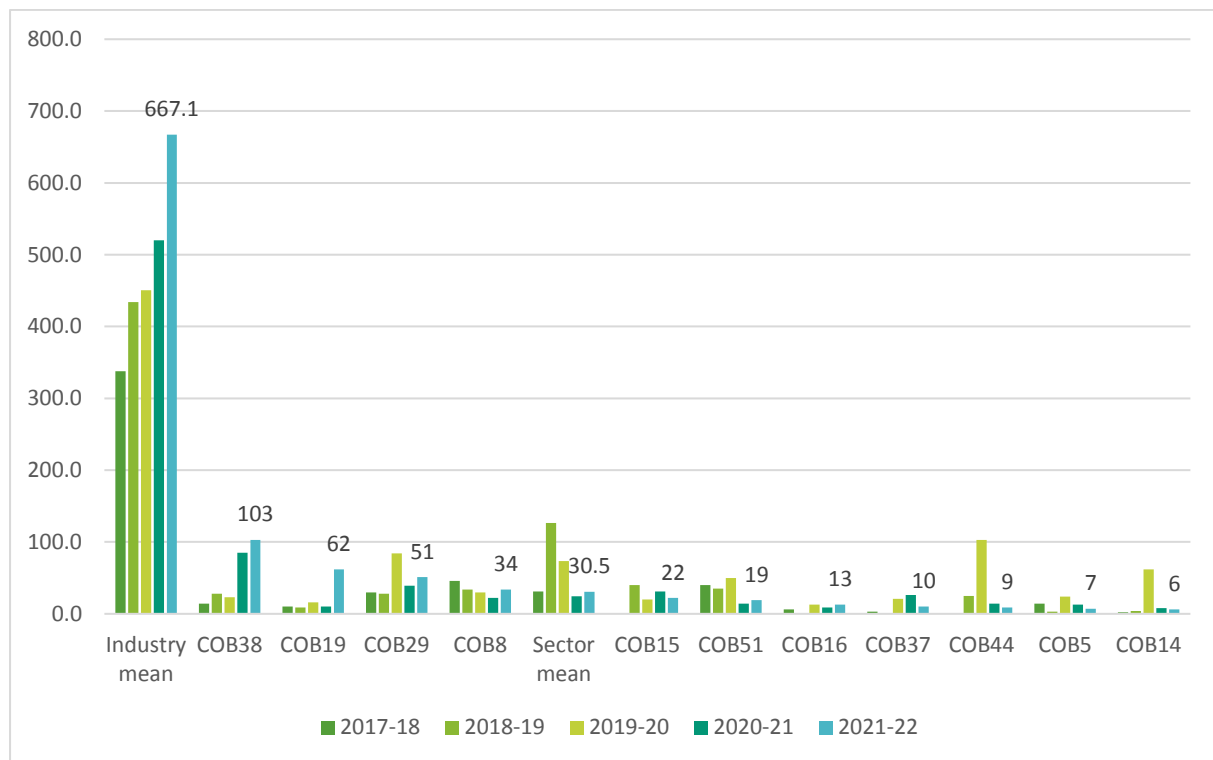


Chart 20: Self-reported complaints per subscriber in Category E

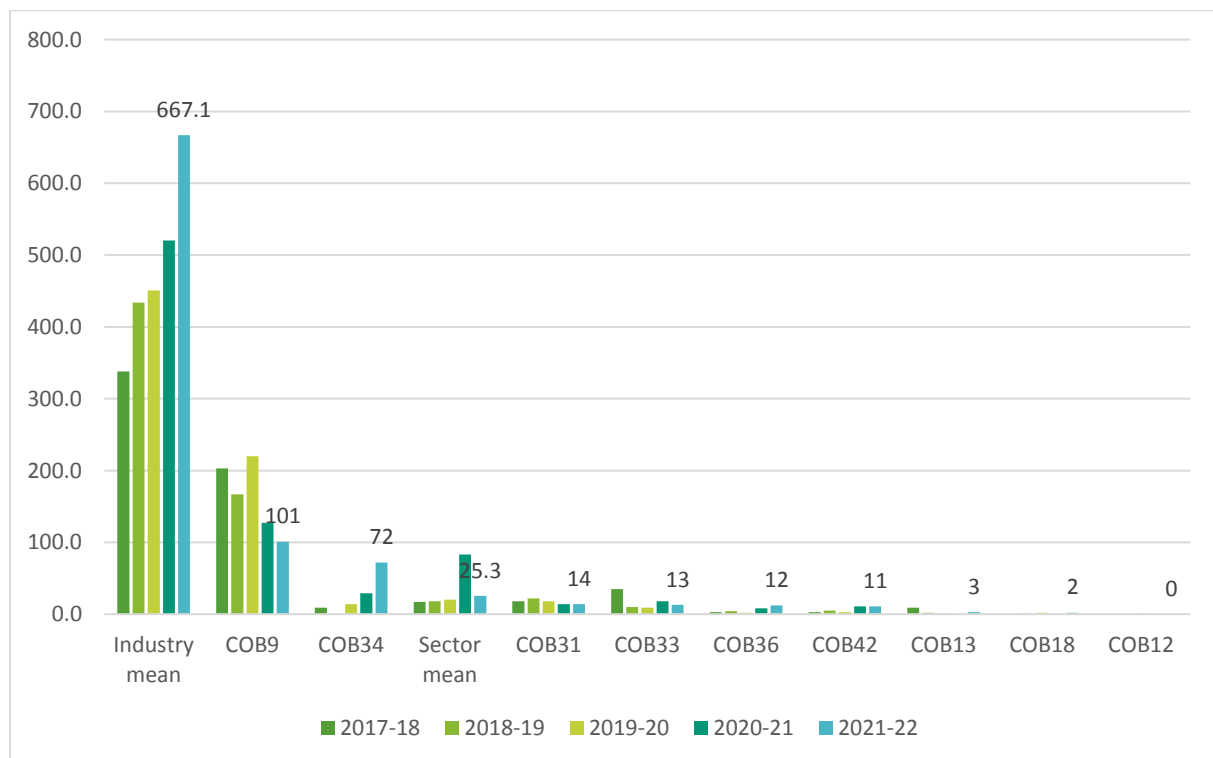
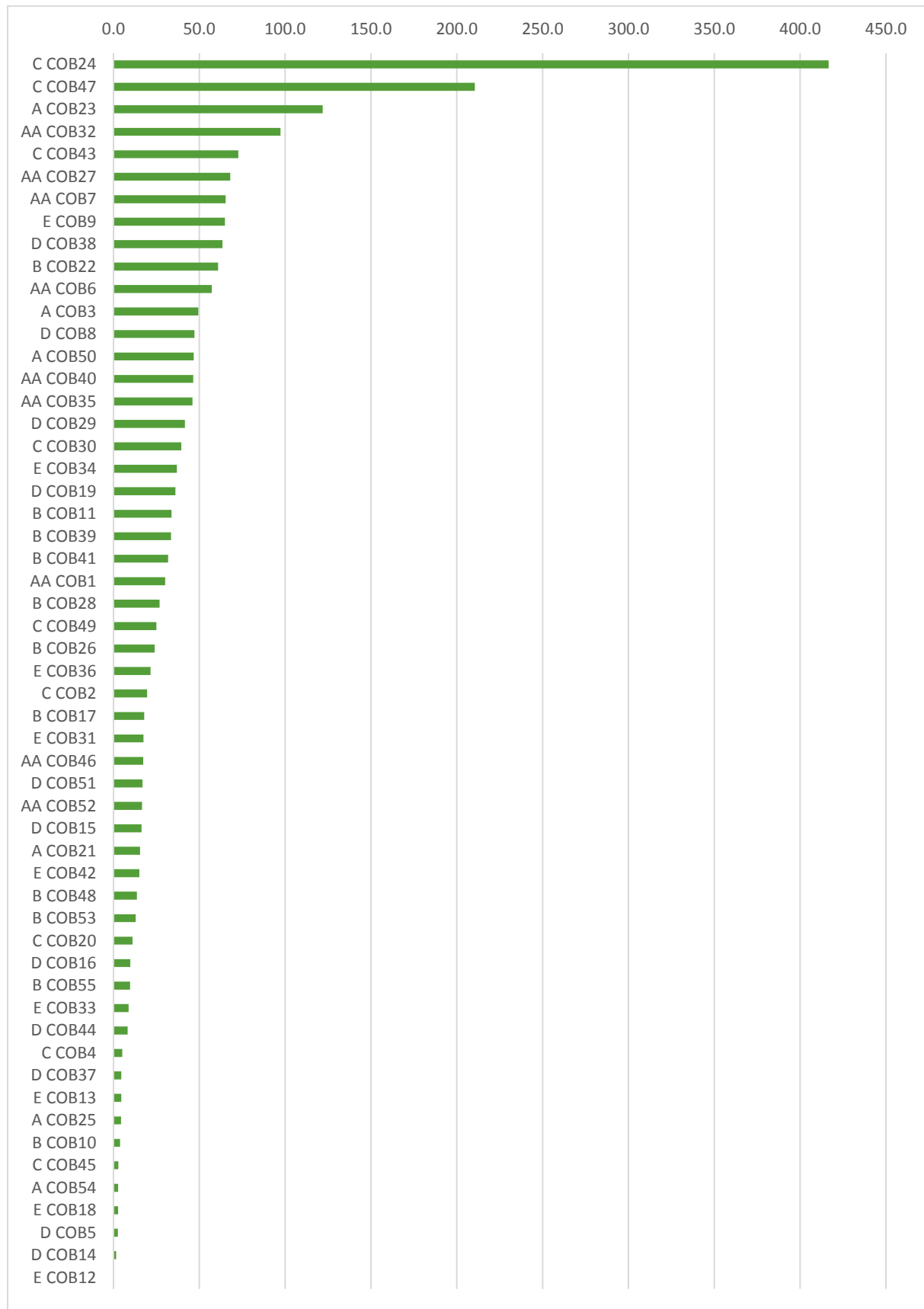


Chart 21: Self-reported complaints per 10,000 accounts in 2021-22



Breaches by specific Code obligations

Table 18: Nature of breaches by Code obligations

	Breach nature	2022 Code sections	2018 Code sections
Delivering on our Promises How we inform you about our products	Key Promises [use only in exceptional circumstances]	A1-A7	KP1-KP10
	Advertising and promotion	B1-B5	D1
	Information about products	B6-B8	D2, D18.1
	Fair Terms and Conditions	B9-B12	D4
Our customer service standards	Training Staff	B13-B14	E2
	Communication	B15-B16	D15
	Inclusive banking services	B17-B25	No reference
	Vulnerable customers	B26-B27	No reference
	Complaints resolution	B28-B34	D27, D28, D29
When you have an account with us	Account statements and balances	B35-B41	D16
	Changes to account	B42-B46	D17
	Term deposits	B47	No reference
	Cheque accounts	B48	No reference
	Joint accounts	B49-B50	D9
	Subsidiary cards	B51-B52	D10
	Closing accounts	B53-B56	D22
	Third party products and services	B57-B58	D13
	Consumer credit insurance	B59-B64	No reference
	Electronic communication	B65-B68	D18
	Replacement of documents	B69-B75	D19
Our approach to lending	Lending	B76-B77	D6
	Lending to Small Business	B78-B88	No reference
	Credit cards	B89-B94	D7
	Safeguards for co-borrowers	B95-B99	D11
	Safeguards for loan guarantors	B100-B120	D12
	Guarantors directors	B121	No reference
	Lenders mortgage insurance	B122-B125	No reference
Our approach to fees, rates and commissions	Interest rates, fees and charges	B126-B133	D3, D5
	Exchange rates and commissions	B134	No reference
Support for customers experiencing financial difficulty	Financial difficulty	B135-B143	D24
	Working with representative	B144-B145	D25
	Debt collection	B146-B156	D26
Our approach to payments	ePayments Code	B157	B
	Direct debit	B158-B162	D20
	Chargeback	B163-B167	D21
Our commitments to your privacy and security	Privacy	B168-B172	D23
How we promote the Code	Publicising Code	B173	E1
How the Code is administered	Compliance responsibilities	C180-C184	E16, E17, E19, E20
	Reverse Mortgage loans	n/a	D8

About the Code

The [Customer Owned Banking Code of Practice](#) (the Code) sets standards of good practice. Subscribers to the Code voluntarily commit to complying with its provisions when dealing with current and prospective customers. The Code is an important part of the broader national consumer protection framework and financial services regulatory system.

The Code is owned and published by the industry advocate for Australia's customer owned banking sector: the [Customer Owned Banking Association](#) (COBA).

The 2014 Code commenced on 1 January 2014 and replaced the 2010 Mutual Banking Code of Practice.

The Code was revised effective on 1 July 2016 to accommodate changes that ASIC made to [Regulatory Guide 221 Facilitating digital financial services disclosures](#) and the *e-Payments Code*. A further update was published, effective 1 January 2018.

Following a review of the Code that began in 2018, COBA developed a [new Code](#) which came into effect on 31 October 2022.

The 2022 Code has more stringent obligations for inclusive banking services, expanded lending obligations and guarantor protections, and greater support for customers experiencing vulnerability.

About the Committee

The Code is monitored and enforced by the independent [Customer Owned Banking Code Compliance Committee](#) (the Committee). The Committee works with stakeholders to improve compliance with the Code and promote good practice.

The Committee offers regular guidance to help subscribers understand and meet their Code obligations.

The [Australian Financial Complaints Authority](#) (AFCA) provides the Committee with monitoring and administration services by agreement. AFCA has appointed a dedicated staff within its office (the Code team) to undertake these duties.

For more information about the Code, the Committee or the Code Team, please visit www.cobccc.org.au.