



ANNUAL DATA REPORT

A companion report to the Insurance Brokers Committee's Annual Report 2020–21 published in August 2021, including detailed analysis of the data, along with observations, guidance and recommendations on improved compliance and better practice.

December 2021

1 January to
31 December
2020

About this Report

This Report is a companion report to the Insurance Brokers Code Compliance Committee's Annual Report 2020–21 published in August 2021. It includes detailed analysis of the findings of the 2020 Annual Compliance Statement (ACS) Verification Program and the Committee's observations on the overall compliance of the insurance broking sector with the Insurance Brokers Code of Practice (the Code), along with guidance and recommendations on how subscribers can improve their compliance reporting and achieve better practice within their organisation.

Contents

MESSAGE FROM THE CHAIR	3
Better compliance requires a cultural shift	3
Appreciation	4
ABOUT THIS REPORT	5
Methodology	5
Guidance for future reporting	6
BREACH DATA KEY FINDINGS	8
More Code breaches but fewer subscribers reported them	8
Over half of all Code subscribers reported nil breaches	9
The top six breach areas for 2020	10
DETAILED BREACH DATA BY CODE SERVICE STANDARD	12
Service Standard 1: Legal standards	12
Service Standard 2: Conflict of interest	13
Service Standard 3: Who we act for	13
Service Standard 4: Scope of covered services	14
Service Standard 5: Acting diligently, competently, fairly and with honesty and integrity	14
Service Standard 6: Remuneration	19
Service Standard 7: Money handling	19
Service Standard 8: Training staff and authorised representatives	20
Service Standard 9: Responding to disasters	21
Service Standard 10: Dispute resolution	21
Service Standard 11: Promoting the Code	22
Service Standard 12: Professionalism	22
THE ROOT CAUSES AND IMPACT OF BREACHES	24
People-related issues were the root cause of most breaches	24

Code breaches impacted almost 21,000 clients	25
COMPLAINTS DATA KEY FINDINGS	27
Top products involved in complaints.....	27
Top issues involved in complaints.....	28
Top outcomes involved in complaints	28
Complaint resolution timeframes	29
CODE COMPLIANCE AND MONITORING ACTIVITIES.....	31
Improving processes and procedures to enhance Code compliance.....	31
Monitoring websites to ensure Code compliance	32
CONCLUSION.....	33
APPENDICES	34
APPENDIX A: ABOUT THE CODE	36
APPENDIX B: CODE SUBSCRIBERS	38
APPENDIX C: DATA TRENDS	40
APPENDIX D: SELF-REPORTED BREACH DATA	47
APPENDIX E: ROOT CAUSE AND IMPACT OF SELF-REPORTED CODE BREACHES IN 2020	50
APPENDIX F: SELF-REPORTED COMPLAINTS DATA	54
APPENDIX G: COMPLIANCE MONITORING ACTIVITIES IN 2020	59

Message from the Chair

I am pleased to present the 2020 Annual Data Report of the Insurance Brokers Code Compliance Committee (the Committee).

The Annual Data Report supplements our 2020–21 Annual Report and 2020 Benchmark Report, which provided readers with an initial summary of Code subscribers' self-reported breach and complaints data. Here, we present a detailed examination of the findings of the 2020 Annual Compliance Statement (ACS) Verification Program – the cornerstone of the Committee's compliance monitoring program.

The discussions we have with Code subscribers as part of the ACS Verification Program don't just allow us to substantiate the self-reported data. They also present us with an invaluable opportunity to examine the stories behind the numbers – the 'why' alongside the 'what' in relation to subscribers' breach and complaints reporting and compliance monitoring – and to gain a greater understanding of the challenges facing individual subscribers and the insurance broking industry as a whole.

These discussions have helped shape the content of this report, enabling us to provide in-depth coverage of subscribers' reporting of Code compliance, along with examples of better industry practice, and guidance and recommendations from the Committee on areas where the reporting indicates that Code compliance could be improved.

Better compliance requires a cultural shift

The theme of our Annual Report was 'Culture is the Key' to compliance. In my Chair's message for that report, I wrote about the Committee's expanded focus on the culture and behaviour of insurance brokers as the key to delivering Code compliant outcomes to clients and others. It is, our intention to deliver compliance improvements by helping create positive shifts in the company culture of our subscribers.

It is clear from some of the findings in this Annual Data Report that such a focus will indeed be required. Although we saw the overall number of Code breaches increase by 66% on the previous year, the number of Code subscribers self-reporting breaches fell to 44% in 2020, down from 51% in 2019. Put another way, 56% of Code subscribers failed to report any breaches whatsoever, including three subscribers in the largest size category.

A similar picture emerged from the self-reported complaints data. While the overall number of self-reported complaints rose by 38% from the previous year, the number of Code subscribers self-reporting complaints dropped from 60% in 2019 to 52%.

As we said in our [Culture is Key Report](#),¹ "...breaches of the Code are not always a bad thing. Lapses and process failures are inevitable, so a breach ultimately means a broker has effective processes in place to identify and pick up issues."

The decline in our self-reported breach and complaints culture is concerning, as it potentially signifies that large numbers of Code-subscribing insurance brokers have compliance frameworks that are failing to detect Code breaches or complaints, or a weak or non-existent self-reporting culture. In the Committee's experience, a subscriber self-reporting nil breaches is unlikely to indicate perfect Code compliance. On the contrary, it is generally an indication that the subscriber

¹ See <https://insurancebrokerscode.com.au/app/uploads/2021/11/IBCCC-OMI-Culture-is-Key-Report-Nov-2021.pdf>.

has an issue with its processes and procedures or that it does not promote an organisational culture that encourages staff to take breach reporting seriously.

Self-reporting enables subscribers to demonstrate a clear understanding of their own compliance performance and their willingness to improve, where necessary. An insurance broking business with a healthy self-reporting culture is one that seeks to provide the best possible outcome for its clients; where the norms and values of the business are aligned with the Service Standards set out in the Insurance Brokers Code of Practice ([the Code](#)). All staff are encouraged to view breach and complaint reporting as an opportunity to learn and improve; and where robust compliance frameworks and processes support each of these things to occur.

“The key is that breaches should ideally be minor and identified and resolved quickly.” ([Culture is Key Report](#))

In the Committee’s experience, a subscriber self-reporting nil breaches is unlikely to indicate perfect Code compliance. On the contrary, it is generally an indication that the subscriber has an issue with its processes and procedures or that it does not promote an organisational culture that encourages staff to take breach reporting seriously.

There are numerous insights and recommendations within this report to help Code subscribers improve all aspects of their compliance monitoring and self-reporting culture, and the Committee encourages all Code subscribers to carefully read the learnings, challenges and examples of good practice shared by the 46 insurance broking firms that participated in the ACS Verification Program.

Appreciation

I take this opportunity to thank all participants to the 2020 ACS Verification Program for their willingness to discuss their breach data reporting and their receptiveness to our feedback on ways to improve their Code compliance. The verification conferences provide a good opportunity for the secretariat to meet with a range of staff from our Code-subscribing community, and it was encouraging to see a cross-section of employees represented at the conferences this year, including staff from Legal and Compliance Departments and Claims Departments, as well as Compliance and Risk Managers and other departmental heads.

The Committee looks forward to working with all our Code subscribers and other stakeholders in preparation for the 2021 ACS Program and Annual Data Report.



Michael Gill
Independent Chair
Insurance Brokers Code Compliance Committee

About this Report

The 2020 Annual Data Report is a companion report to the Committee's [Annual Report 2020–21](#)², which was published in August 2021.

Where the Annual Report outlined the Committee's activities and provided a brief snapshot of Code subscribers' self-reported breach information and complaints data, this report contains a detailed analysis of the findings of the 2020 Annual Compliance Statement (ACS) Verification Program – the cornerstone of the Committee's compliance monitoring program.

It also includes the Committee's observations on the overall Code compliance of the insurance broking sector, along with guidance and recommendations on how subscribers can improve their compliance reporting and achieve better practice within their organisation.

Each year, the Compliance Manager undertakes the ACS Verification Program, which includes a series of conferences with a sample group of Code subscribers to validate their breach reporting and gain insights into the day-to-day management of their Code compliance obligations (see 'Methodology', below, for more detail about this). The aim of the program is for the Committee to hear directly from subscribers about:

- the story behind their data
- the context for their reported breach numbers
- how they identify and respond to breaches of the Code
- any emerging trends
- their strategies for improving their overall Code compliance, and
- any examples of good practice that can be shared with the industry.

The program also provides Code subscribers with the opportunity to:

- raise with the Committee any concerns they may have about the ACS process
- receive feedback and guidance from the Committee about completing their ACS
- review and improve their compliance monitoring and breach data reporting, and
- identify any emerging risks or issues.

Methodology

A total of 456 Code subscribers provided self-reported breach and complaints data via the 2020 ACS (covering the period 1 January to 31 December 2020). This included 163 new subscribers to the Code, following the addition of all Steadfast brokers to the Code community in December 2019.³ The ACS verification conferences were conducted with a sample group of 46 subscribers (equivalent to 10% of all Code subscribers) from different sizes and regions:

² See https://insurancebrokerscode.com.au/app/uploads/2021/08/IBCCC_Annual_Report_2020-21-Aug-2021.pdf.

³ See Appendix B, Table 3 for a breakdown of all Code subscribers by state (head office) and size of operation.

Category	ACT	NSW	QLD	SA	VIC	WA	Total
Category A (100+ FTE⁴ staff)	-	3	1	1	4	-	9
Category B (51–100 FTE staff)	-	1	-	-	3	1	5
Category C (31–50 FTE staff)	-	2	-	-	3	2	7
Category D (21–30 FTE staff)	-	1	1	-	3	1	6
Category E (up to 20 FTE staff)	1	3	5	2	6	2	19
Total	1	10	7	3	19	6	46

The conferences provide a good opportunity for the Compliance Manager to meet with a wide range of senior staff from Code-subscribing institutions, including:

- Compliance & Risk Managers
- Account Managers
- Chief Operating Officers
- General Managers
- Operations Managers
- Corporate Counsel and Heads of Compliance
- Managing Directors
- External Compliance / External Auditors
- Claims Managers
- Broker Support Officers
- Administration Managers, and
- Finance Managers.

From the Committee’s viewpoint, we appreciate being able to gain a better understanding of subscribers’ breach data, complaints reporting, monitoring mechanisms and websites, and to provide them with guidance and support in these areas. Subscribers have expressed their appreciation for this feedback and implemented our suggested improvements. It is hoped that the Committee’s guidance and feedback for improving the ACS and breach data reporting process are also shared with institutions’ Boards and Executive Management teams.

Guidance for future reporting

The following advice is based on the Committee’s observations of the ACS, Breach Data Report and conversations with subscribers during the ACS Verification Program. We encourage all Code subscribers to consider this advice when completing the ACS Program in future.

⁴ Full Time Equivalent.

All Code breach information must be entered into the Breach Data Report

Due to the large number of Code subscribers and the immense amount of data gathered as part of the ACS Verification Program, the Committee requires all subscribers to add their Code breach information into the Breach Data Report. The Breach Data Report is a standardised template that enables the Compliance Manager to analyse and run formulae in a standardised way. Where a subscriber has updated its incident register, the Compliance Manager will copy information into the Breach Data Report and verify this with the relevant subscriber.

The ACS is not a form-filling exercise – it is a tool to help Code subscribers assess and fine-tune the robustness of their compliance programs.

The Committee notes that several Steadfast Code subscribers have provided information about incidents via the Steadfast Incident Register rather than the Breach Data Report. If Steadfast subscribers intend to keep using this register, the Committee recommends including a column to assess whether each incident is a Code breach and, if so, which particular Service Standard has been breached.

Ensure breaches reported in the portal match those in the Breach Data Report

The Compliance Manager cross-references the breaches that subscribers report in the portal with the breaches they record in the Breach Data Report. In cases where there is a discrepancy, the Compliance Manager will manually update the breach data in the ACS to match the information in the Breach Data Report.

Use the Breach Data Report to consider compliance

The process of completing the ACS and the Breach Data Report may alert subscribers to ways they can improve their processes and procedures, and thus achieve better compliance with the Code. For example, one Category E subscriber that participated in the ACS Verification Program ensures that the information recorded in the Breach Data Report about immediate and long-term remedial action is also recorded in the subscriber's internal monitoring systems and registers to ensure that it is followed through.

The pros and cons of using an external compliance firm for breach reporting

Several subscribers use external compliance firms to complete their Breach Data Report or set up compliance monitoring frameworks. For example, one Category E subscriber with only three staff members uses an external compliance consultancy firm to monitor all compliance-related incidents. Staff report any incidents to the external consultant, who then monitors and assesses those incidents to determine whether they are a breach of the Code. The external consultant also conducts audits and sets compliance agendas and tasks for the subscriber.

Using an external compliance consultant in this context can work successfully, as long as the subscriber has a healthy

Failing to report a breach is itself a breach of the Code

Discussions with one Category A subscriber that participated in the ACS Verification Program revealed that a breach identified as part of an investigation during the year (2020) was not reported in the subscriber's 2020 Breach Data Report. The subscriber was unaware of this until the Compliance Manager raised it during the ACS verification conference. Upon closer review, the subscriber discovered that the breach was not reported because of a system error in the Code breach register. The subscriber has since addressed the breach and committed to including it in its 2021 ACS, as both the actual breach and the breach caused by the failure to report.

compliance culture that actively encourages staff to self-report incidents, identify emerging risks, and view any non-compliance incidents as an opportunity to learn and improve.

Other subscribers use external auditors to review their Code compliance, reporting any breaches that are identified as part of the auditing process. One Category D subscriber does not track incidents via a breach register, instead relying on an external auditor to identify incidents and breaches in a biannual review. It became apparent during the ACS verification conference that the subscriber misunderstood the difference between an incident and a Code breach. The Compliance Manager subsequently advised the subscriber to add a tab to their Incident Register to track whether any incident is also a breach of the Code.

Utilise the tools and resources on the Committee's website

Our 'Tip of the Month' resource, published on the Committee's website, includes several articles to help subscribers complete the ACS and identify Code breaches. For the 2020 ACS, we published the following "Tip of the Months":

- [2020 Annual Compliance Statement guide⁵](#) (November 2020)
- [It is much more than law and regulation⁶](#) (April 2021), and
- [Breaches should guide the way forward⁷](#) (July 2021).

During the ACS verification conferences, several subscribers told us that the Committee's various guidance resources helped them to better understand and interpret their Code obligations, which in turn helped them to identify and report Code breaches. We strongly encourage all subscribers to review these resources with a view to improving their breach reporting in the future.

Breach data key findings

More Code breaches but fewer subscribers reported them

There were 3,328 self-reported Code breaches in 2020, up from 2,006 the previous year. This marks the sixth consecutive year in which breach numbers have risen.⁸ Despite the increase in overall breach numbers, the volume of subscribers to self-report a breach fell from 51% in 2019 to 44% in 2020, meaning that more than half of all subscribers self-reported nil breaches during the reporting period.

Subscriber influx impacts the breach data

On 1 December 2019, the National Insurance Brokers Association (NIBA) welcomed all Steadfast brokers to the Code community, resulting in a 56% increase in subscriber numbers. This year was the first time these new subscribers were required to participate in the ACS Program – and the first opportunity for them to familiarise themselves with the requirements of our monitoring program.

Consequently, it is difficult to meaningfully compare the 2020 data with that of previous years. However, as new subscribers adapt to their new self-reporting obligations over the coming year, the Committee is confident our compliance monitoring will become increasingly accurate and insightful.

⁵ See <https://insurancebrokerscode.com.au/2020-annual-compliance-statement/>.

⁶ See <https://insurancebrokerscode.com.au/it-is-much-more-than-law-and-regulation/>.

⁷ See <https://insurancebrokerscode.com.au/breaches-should-guide-the-way-forward/>.

⁸ See Appendix C, Chart 1.

The highest proportion of self-reported breaches came equally from the largest and the smallest group of Code subscribers: together, Category A and Category E subscribers accounted for almost two-thirds of all breaches (32% each). At the other end of the spectrum, Category B subscribers accounted for just 8% of all Code breaches, while Category C self-reported 14% and Category D 13%.

Traditionally, Code subscribers from Category A have had the strongest self-reporting culture: in recent years we have seen more subscribers in the largest size category self-report a Code breach than any other size category. In 2020, however, Category C subscribers had the highest self-reporting rate, with almost 85% of organisations in that size category reporting a Code breach – an increase of 11% on 2019. Around 82% of Category A subscribers self-reported a Code breach, while only 34% of Category E subscribers did the same.⁹

Over half of all Code subscribers reported nil breaches

A total of 238 Code subscribers self-reported nil Code breaches in 2020. Of these, 215 were subscribers in Category E; however, as was the case in 2019, three subscribers in Category A also reported nil breaches.¹⁰ During its ACS verification conference, one of these Category A subscribers explained that it identifies breaches of the Code through its complaints data, as well as relying on the industry experience and ‘common sense’ of its staff to detect breaches. The subscriber confirmed, however, that there is no benchmarking in place. When new staff members come on board, they are given an employee handbook and expected to acquaint themselves with the organisation’s processes and procedures.

Despite reporting the second highest number of Code breaches for the year, more than two thirds of all Category E subscribers reported nil breaches. While subscribers in this category almost doubled following the addition of all Steadfast members in 2019, this does not fully explain why so few of the smallest Code subscribers did not report a single Code breach.

Several of these Category E subscribers were quizzed during their ACS verification conferences about why they had reported nil Code breaches. Discussions with one subscriber revealed some confusion about how to identify and report a Code breach. The subscriber purely relied on the industry association training program on how to identify a Code breach. To assist the subscriber to improve its internal compliance going forward, the Compliance Manager has provided it with information on how to detect and record a Code breach.

Another Category E subscriber that reported nil breaches explained that it has a positive culture of compliance, whereby staff know how to identify a Code breach and are able to report breaches and complaints to the Director, who has an ‘open door’ policy. There is also an incident register that is monitored by a designated staff member, although it does not have the capacity to flag Code breaches. Nonetheless, the subscriber is confident that there have not been any Code breaches to date.

Breaches reported to ASIC and OAIC

During 2020, Code subscribers reported 21 breaches to the Australian Securities and Investments Commission ([ASIC](#)) and five breaches to the Office of the Australian Information Commissioner ([OAIC](#)).

⁹ See Appendix C, Chart 2.

¹⁰ See Appendix D, Table 12.

Does your organisation promote a culture of compliance?

As we have consistently stated in previous Annual Reports, the Committee is concerned that Code subscribers are not identifying and reporting all breaches. Rather than indicating Code compliance, nil breaches or low breach numbers potentially signify, at best, inadequate processes and procedures for detecting and reporting breaches, and, at worst, an organisational culture that discourages self-reporting of breaches or complaints.

We strongly encourage subscribers that reported nil or low numbers of Code breaches or complaints to assess their frameworks and review their compliance culture. Use the Code as a tool for monitoring any issues or errors that may be occurring within the business. Map all incidents against the Code's Service Standards to determine any Code breaches. Encourage staff across the organisation to report breaches and complaints and help them to see that self-reporting is an opportunity to learn, to improve and to provide better outcomes for clients.

The top six breach areas for 2020¹¹

- As was the case in 2019 the two most breached areas of the Code were Service Standard 5 (49% of all Code breaches¹²), which sets standards of client service to buying insurance, and Service Standard 1 (22%), which covers compliance with legal obligations.
- Service Standard 7, which relates to money handling, was the third most breached area in 2020, accounting for 11% of all Code breaches (up from 7% in 2019).
- The fourth most breached Code standard was Service Standard 12, which is designed to ensure that Code subscribers do not bring the insurance broking profession into disrepute.
- 5% of all Code breaches were reported in Service Standard 4 (Scope of covered services), which saw it fall from the third most breached area in 2019 to the fifth most breached area in 2020.
- Breaches of Service Standard 8 (Training) remained similar to 2019, accounting for 3% of all Code breaches.

More in-depth analysis about the self-reported breach data for each of the 12 Code Service Standards can be found in the next chapter.

¹¹ Appendix C, Chart 3.

¹² Service Standard 5 was split into three sections for the 2020 ACS Program: buying insurance (referred to in this report as Service Standard 5.1); claims handling (Service Standard 5.2); and acting for the insurer (Service Standard 5.3).

Code breach or complaint?

It is important for subscribers to distinguish between a Code breach and a complaint. Code breaches refer to the individual aspects of the Insurance Brokers Code of Practice and relate to non-compliance with one or more of the Code's 12 Service Standards. They can be identified numerous ways, including through complaints, internal or external audits, and self-reported by staff.

Definition of Breach

A failure to comply with the obligations of the Code in relation to the provision of an insurance broking service (defined with reference to the ASIC Regulatory Guide 78 – Breach Reporting by AFS Licensees, the Australian Standard AS 3806 2006 – Compliance Programs, Section 912D of the Corporations Act 2001).

Definition of Complaint

[An expression] of dissatisfaction made to or about an organisation, related to its products, services, staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required (as per AS/NZS 10002:2014).

Identifying Code breaches via complaints

Where complaints are used to identify Code breaches, subscribers may use an incident register which tracks all complaints – however, they should also have in place a process for identifying whether an individual complaint gave rise to a Code breach.

Identifying a Code breach should not be undertaken as a 'passive' or incidental exercise alongside a complaints review. Subscribers should ensure that their processes for detecting and reporting Code breaches via incident or complaints registers are robust enough to capture all breaches, in addition to having other breach detection methods in place.

Detailed breach data by Code Service Standard

This chapter provides a detailed analysis of the self-reported data for each of the 12 Code Service Standards.¹³ It is based on discussions with 46 Code subscribers of varying sizes as part of the ACS Verification Program and aims to provide insights into why some subscribers self-reported high numbers of breaches of certain areas of the Code.

Service Standard 1: Legal standards

Service Standard 1 ('We will comply with all relevant law') was the second most breached Code standard in 2020, with 22% of all Code subscribers self-reporting a total of 718 breaches. Most of these subscribers (58 out of 95) self-reported no more than four breaches each. At the other end of the spectrum, however, one Category A subscriber self-reported 99 breaches of Service Standard 1 and a Category D subscriber self-reported 83 breaches.

Of the 254 Service Standard 1 breaches self-reported by Category A subscribers, more than half (55%) came from just two brokers, including the broker that self-reported 99 breaches and another that reported 41 breaches.

The broker that self-reported 99 breaches explained to the Compliance Manager that all breaches related to the conduct of its authorised representatives, and provided the following as examples of why the breaches occurred:

- the Financial Services Guide (FSG) was not published on the broker's website
- emails were forwarded to the wrong party
- authorised representatives used others' staff login details when onboarding staff, and
- client information was retained without permission or knowledge.

As a result of the breaches, and to prevent a recurrence in the future, the broker has conducted extensive training – particularly around privacy issues – to ensure that its staff and authorised representatives understand their legal obligations under the Code.

The Category A subscriber that reported 41 breaches explained that one breach had a particularly high customer impact. The breach was the result of a cyber-attack on the subscriber's IT system, which sent a phishing email to over 1,700 clients asking them to click on a link to access documents. The subscriber took immediate action by securing the impacted account, working with the broker's cyber security team to trace the email, and directing the legal team to notify all affected parties. Longer term remediation included resetting passwords across all user accounts and creating a two-factor authentication system for accessing emails outside the subscriber's server.

Only five Category B subscribers self-reported breaches of Service Standard 1, with just two self-reporting more than four breaches. One subscriber self-reported 18 breaches after separate emails were sent to the wrong clients. The breaches impacted a total of 30 clients – 15 clients who received the email in error, and 15 clients for whom the emails were originally intended.

The subscriber noted that email phishing scams are becoming more prevalent, and to combat this, it has ramped up IT training to teach staff about the dangers of clicking on suspicious links within emails. The subscriber also conducts two mandatory training sessions a year to address privacy-

¹³ See Appendix D, Table 13.

related breaches, and regularly shares information with staff across the organisation via ‘town hall’ meetings.

More than half (58%) of all Category C subscribers self-reported at least one instance of non-compliance with the Code’s legal obligations standard, although most (13 out of 19) reported fewer than five breaches in total.

One Category C subscriber explained that all 12 of the Service Standard 1 breaches it reported were the result of errors in emails caused by, for example, automated completion of email addresses or lack of attention by staff when sending out emails. The subscriber has taken remedial action that includes educating staff about privacy laws and reminding staff in team meetings to take care when emailing clients. Procedures have also been changed so that a manual check of attachments is conducted prior to sending emails.

While around a third of all Category D subscribers self-reported a breach of Service Standard 1, more than three-quarters (77%) were reported by just two brokers – one which accounted for 83 breaches and the other which accounted for 30 breaches.

Service Standard 2: Conflict of interest

Under Service Standard 2, subscribers must appropriately manage any conflicts of interest that arise between them and their clients. In 2020, five subscribers self-reported a total of 10 breaches of this service standard. Four of these subscribers (one each in Categories C and D, and one in Category E) reported a single breach, while the six remaining breaches were reported by one Category A subscriber.

According to the Category A subscriber, all six breaches occurred when the details of one client were mistakenly emailed to another client. During the ACS verification conference, the subscriber acknowledged that these breaches could have been reported as privacy breaches, covered under Service Standard 1. However, the subscriber explained that because both clients work in the same industry, the subscriber considered the breaches to be a conflict of interest, and therefore a breach of Service Standard 2.

Service Standard 3: Who we act for

Five subscribers (one each in Categories A and C, and three in Category E) reported a single breach of Service Standard 3 (‘We will clearly tell you we do not act for you’).

According to the Category A subscriber, the breach occurred when its authorised representative sent a quote slip with the incorrect Australian Financial Services Licence (AFSL) information to one of the subscriber’s clients. Investigating the breach, the subscriber found that some of the information in the representative’s standard template was incorrect. The representative subsequently updated the template, and the subscriber has since implemented a program, built into its compliance calendar, to regularly review the templates of all its authorised representatives.

In the case of one of the Category E subscribers, its breach of Service Standard 3 was identified by an external auditor, which found issues with some of the information published on the broker’s website. As well as failing to include a link to the Insurance Brokers Code of Practice, the website contained the contact details of a staff member who no longer worked for the organisation. In its ACS verification conference, the subscriber advised that it would update the website to include the correct contact information and a link to the Code.

Service Standard 4: Scope of covered services

Service Standard 4 – which stipulates subscribers clearly advise clients about the scope of the insurance services they cover – was the fifth most breached Code standard in 2020. With 150 breaches self-reported by 43 subscribers, this service standard accounted for 5% of all self-reported breaches for the year. While 39 out of 43 subscribers self-reported fewer than 10 breaches of Service Standard 4, the remaining four subscribers (three Category A and one Category B) self-reported 10, 12, 17 and 21 breaches respectively.

One of the Category A subscribers reported a single incident resulting in 10 breaches that impacted 10 clients. The breaches were due to the subscriber's diary system¹⁴ not being appropriately actioned. This meant that the diary system was unable to verify the disclosure date and resulted in clients not being sent an FSG. The subscriber remediated the breaches by posting hard copies of the FSG to the affected clients.

Another Category A subscriber reported 12 breaches that impacted 12 clients. The breaches were the result of clients either not receiving an FSG and/or a Product Disclosure Statement (PDS) or receiving the wrong FSG/PDS. Upon identifying the breaches, the subscriber sent the correct documents to all affected clients and has undertaken implementation of a new administrative support process to prevent similar breaches from occurring in the future.

A third Category A subscriber self-reported 17 breaches of Service Standard 4, with causes including:

- failing to issue clients with a PDS
- sending incorrect documents to clients
- entering an incorrect expiry date into the system, and
- allowing a policy to lapse incorrectly.

The Category B subscriber that reported 21 breaches of Service Standard 4 provided a range of breach causes, including:

- failing to include details of the authorised representative in the FSG
- failing to provide clients with the statement of advice
- failing to remove information from the PDS that no longer applied, and
- failing to update the FSG with relevant information.

Service Standard 5: Acting diligently, competently, fairly and with honesty and integrity

Service Standard 5 is the longest and most detailed section of the Code. It covers behavioural standards that subscribers must adhere to when a client purchases insurance and/or makes a claim, and when the subscriber acts on behalf of the insurer rather than the client. In 2020, 49% of all breaches reported by subscribers were of this Code standard, making it the most breached standard overall for the fourth consecutive year.

Given the broad range of breaches that can occur against Service Standard 5, the Committee split it into three subsections for the 2020 ACS to make it easier for subscribers to categorise and learn from their Service Standard 5 breaches: one for breaches of the 'buying insurance' aspects of the

¹⁴ A diary system is an internal flag that captures the activities of insurance brokers.

standard; one for breaches of claims handling; and one for breaches relating to behaviour when acting on an insurer's behalf.

Service Standard 5.1: Buying insurance

Non-compliance with the Code's standard relating to buying insurance was by far the most breached area of the Code. With 1,617 breaches self-reported by 115 subscribers, breaches of this standard accounted for 46% of all Code breaches in 2020. More than half of all Code subscribers in categories A to D reported at least one 'buying insurance' breach, while only 17% of subscribers in the smallest size category did the same. Most subscribers (56%) reported fewer than 10 breaches. Seven subscribers reported more than 100 breaches each; however, these high numbers are largely attributable to delays in issuing renewal notices within 14 days (see the box below for more information about this) and the fact that these subscribers recorded each policy affected as a separate breach.

Sending late renewal notices is not always a breach of Service Standard 5

Unlike Section 58 of the Insurance Contracts Act (ICA), which stipulates that policy holders must be notified no later than 14 days before the day on which their policy expires, the Insurance Brokers Code of Practice makes no reference to specific timeframes for providing clients with renewal notices. The relevant advice in Service Standard 5 of the Code states:

When you are buying insurance and we act on your behalf, we will do the following (unless we agree with you or tell you otherwise):

- *receive all general insurance notices from the insurer on your behalf and pass the notices or relevant information in the notices to you promptly (including but not limited to renewal information where relevant).*

The Committee acknowledges that failure to provide a client with at least 14 days' notice of the expiration of their insurance policy and the terms for renewing the policy may be a breach of Section 58 of the ICA. However, as the Code makes no mention of a specific timeframe for providing clients with renewal notices, we would not expect subscribers to report this as a breach of Service Standard 5 of the Code. If a subscriber can demonstrate, through evidence such as detailed file notes, that it has done everything possible to fulfil its obligations to both the insurer and the client regarding the provision of renewal notices within a timely manner, then the subscriber will be considered to have met its obligations under Service Standard 5 of the Code.

For example, in 2020 a Category E subscriber self-reported 143 instances of non-compliance with the Code's standard relating to buying insurance because 143 clients received their renewal notices less than 14 days before the policy was due to expire. During the ACS Verification Program, the subscriber revealed that it was not to blame for all the delays. In some instances, delays were caused by the underwriter not providing the subscriber with the revised terms of the renewal, or by property managers not completing their reviews in a timely manner. In other instances, there were issues with the insurer's IT system, or the client was slow to provide the subscriber with requested information. Provided the subscriber could show evidence that it had communicated with the client and the insurer in a timely manner about the renewal of the client's policy, it did not need to report all late renewals as a breach of Service Standard 5 of the Code.

Subscriber tip

Where renewal notices are sent to clients less than 14 days before their policy is due to expire, subscribers should review each case to determine why. Are the delays due to a particular insurer being slow to provide renewals? Or a particular client being slow to provide requested information? Answering these questions can pre-empt and help resolve issues before they result in further delays.

'Buying insurance' breaches caused by sending renewal notices late

There were some self-reported breaches of Service Standard 5.1 that were found to be actual Code breaches. One Category A subscriber self-reported 162 'buying insurance' breaches, 90% of which were the result of failing to send clients their renewal notices within 14 days and sending out Section 58 letters that included incorrect policy numbers. The subscriber explained that it had implemented a new process for sending out client renewal notices that included sending out Section 58 letters, as the broker was no longer offering renewals. In the cases where the Section 58 letters included the wrong policy number, the subscriber contacted each client within 14 days. The Code breaches impacted 1,174 clients.

A Category E subscriber self-reported 23 'buying insurance' breaches that related to renewal notices being sent out late. In each instance, the delay was caused by the subscriber's staff failing to update clients about their policy renewals. Upon identifying the issue, the subscriber updated its policies and procedures to include a fortnightly report to all brokers, advising them when clients' policies are due for renewal and alerting them to issue renewal notices.

In the case of one Category D subscriber, 10 of its 14 self-reported breaches of Service Standard 5 related to delays in sending out renewal notices to clients. Reasons for the delays included staff being on leave, clients requesting that the policy be sent with another policy, and clients requesting separate renewal notices for multiple policies.

'Buying insurance' breaches caused by other issues

Other breaches of Service Standard 5.1 were caused mainly by human or system error. One Category A subscriber self-reported 93 'buying insurance' breaches, which consisted of three separate incidents impacting 93 clients. All three incidents were the result of the actions of authorised representatives.

In one case, the authorised representative had not correctly processed several policies, leaving clients without the appropriate cover. The issue was identified via brokers running a report using the correct process or by the insurer or the client querying the renewal with the broker. The authorised representative was advised of the error and given assistance to fix it.

Using the Committee's guidance resources to good effect

Despite not having previously recorded a single Code breach, one Category E subscriber self-reported multiple breaches of the Code's 'buying insurance' obligations in 2020. Having reviewed several of the Committee's guidance resources, including previous Annual Reports and webinars on breach identification, the subscriber's staff were able to gain a better understanding about what constitutes a breach of Service Standard 5 and improve Code compliance overall.

In another case, when running a renewal report the subscriber discovered that the policy was missing from the renewal and had not been processed in the authorised representative's system. The issue was caused by a system migration policy that was not captured on the report.

In the third instance, the authorised representative mistakenly cancelled a number of policies. The breach came to light after the insurer and/or the client enquired about the renewal status of the policy and the subscriber realised that there was no cover. The subscriber instructed the authorised representative to undergo appropriate training and implement adequate processes to prevent a recurrence.

In one breach reported by another Category A subscriber, cover under a motor vehicle policy placed the agreed value of the vehicle at approximately \$150,000. In entering the agreed value into the system, however, the broker input the wrong amount. The vehicle was written off in an accident and the client made a claim through the insurer. The error was identified during the claims process and the client was compensated. The breach had an overall financial impact of more than \$11,000.

A third Category A subscriber self-reported nine instances of non-compliance with the Code's buying insurance standard (although it was established during the ACS verification conference that there were nine policies with only two clients impacted). The breaches occurred when the subscriber failed to include plumber's liability insurance on clients' policies when they were renewed. Two clients subsequently lodged claims for plumber's liability insurance and the subscriber was notified of the breaches when it received a claims notification. The subscriber audited more than 1,000 client files to determine whether any other clients were missing plumber's liability cover and confirmed that only the two identified clients were impacted by the breach.

The importance of recording file notes

A Category E subscriber reported a breach of Service Standard 5.1 that was caused by a lack of file notes about a client's insurance policy.

After their premises was broken into, the client lodged a claim which was denied because the policy did not include cover for money stored in a safe or strong box. The client challenged the claim decision.

As the subscriber could not produce any file notes to indicate that the client had not chosen to take out this cover, the subscriber opted to make an ex-gratia payment to cover the client's losses.

Service Standard 5.2: Claims handling

There were 66 breaches of Service Standard 5 relating to claims handling (2% of the total), reported by 29 subscribers. A third of the breaches were reported by subscribers in the largest size category, with one Category A subscriber accounting for 13 breaches – around one in every five.

Breach examples provided by this Category A subscriber during its ACS verification conference included failing to advise the client of the policy's legal costs limit, failing to fulfil the client's request for management liability insurance cover, and causing delays to the claims handling process. All of these breaches were identified through client complaints and have resulted in the subscriber implementing long-term remedial action designed to improve claims handling timeframes.

Another Category A subscriber reported four breaches. One occurred when a broker placed incorrect cover for a client, which led to the client's claim being denied. The issue of cover has since been resolved by the client and the underwriter. The broker was provided with appropriate training in the correct processes and procedures, and the subscriber conducted a risk review of its brokers to ensure that all clients have been provided with the correct cover.

A second breach occurred when an authorised representative placed cover for a client using an incorrect address. Although the client did not make a claim, the breach was identified when an underwriter examined why there were so many vehicles at the same address. The contract with the authorised representative was eventually terminated due to behavioural issues, and the subscriber reviewed the representative's client files to determine any other incidents and issues.

One Category E subscriber reported three claims handling breaches, one of which occurred because a broker failed to pass a client's invoices for outstanding claims onto the claims manager. The breach came to light after the client queried the status of the claims. Manual error was identified as the root cause of the breach, with the broker accepting responsibility, resolving the issue with the client and the underwriter, and undertaking appropriate training.

Service Standard 5.3: Acting for the insurer

The third aspect of Service Standard 5, which relates to a subscriber's conduct when they act on behalf of an insurer rather than a client, was the subject of 31 breaches (1% of the total), self-reported by seven subscribers (three in Category E and one in each of the other size categories).

Two-thirds of all breaches were attributed to one Category C subscriber that was acting for the insurer at the time. Three of the breaches occurred when automated renewal reminders were not sent to clients 30 days prior to the policy expiring. The reminders were supposed to be emailed automatically from an online system maintained by a third-party provider. The breaches were identified by the subscriber's compliance manager conducting a manual check and rectified by manually sending out the renewals to clients.

One Category A subscriber reported a breach that affected six professional indemnity policies under a binder agreement. Due to an issue with the online quote system, clients were provided with quotes that mistakenly included an extra month's coverage in the policy. The product owner reissued the policies and honoured the additional month of coverage, while the system error was fixed and monitored.

IT issues also caused a breach at a Category E subscriber when an authorised representative's document management system failed to protect data during a file transfer. In the subscriber's view, human error was also to blame, as the existing broker did not know how to ensure that data was protected when transferring files.

The same subscriber also reported an instance of a client not receiving a renewal notice/invoice 14 days prior to the due date as a breach of Service Standard 5.3. As previously mentioned, the Committee notes that this is a breach of the law, not a breach of the Code.

Using information from denied claims to better advise clients

One Category D subscriber monitors and reviews all denied claims as a way of identifying problematic clauses within insurance policies or problematic insurance providers. The subscriber uses the information about denied claims to pre-empt issues with existing clients' claims and when advising potential clients about particular policies and insurers.

Service Standard 6: Remuneration

Service Standard 6 requires subscribers to be transparent with their clients about whether and how they are remunerated for providing covered services. A total of 50 remuneration-related breaches were self-reported by 25 subscribers in 2020. Between them, 16 Category E subscribers accounted for more than half (56%) of the breaches, while comparatively few subscribers in the other categories recorded Service Standard 6 breaches (two Category A subscribers, one Category B subscriber, and three subscribers each in Categories C and D).

While most subscribers' breach numbers totalled three or less, one Category C subscriber self-reported 10 remuneration-related breaches. During the verification conference, the Compliance Manager ascertained that these 10 breaches shared a single root cause (remuneration amounts, and conflict of interest disclosures were not provided as part of the advice to clients) and should have been reported as one breach that impacted 10 clients. The subscriber has since provided appropriate training to the relevant brokers.

Failure to disclose or clearly explain the broker fees to clients when they purchase insurance policies was a common cause of many Service Standard 6 breaches. After discovering that a client had not been advised about the broker fee, a Category E subscriber had to refund the fee to the client and implement more frequent staff training around broker fees. One Category A subscriber recorded two breaches that came to light after clients cancelled their insurance policies. In both cases, the clients had not been advised that the broker would retain its fees if they cancelled the insurance policy. The clients were subsequently refunded the fees. The same subscriber recorded a third breach after a processing error caused a client to be charged a broker fee of \$3,000 instead of \$300. The client was refunded \$2,700.

In the case of one Category E subscriber, its FSG included incorrect advice about the rate of commissions for insurers. The breach was identified by an external compliance provider and the subscriber corrected the advice and discussed the issue with its staff.

Service Standard 7: Money handling

Subscribers' obligations relating to how they must handle any money received from clients are set out in Service Standard 7. It is concerning to note that breaches relating to money handling have continued to rise each year since 2017.¹⁵ In 2020, more than one in every 10 self-reported breaches involved money handling issues, with 370 breaches reported by 64 Code subscribers. This made it the Code standard with the third highest number of breaches for the year.

While there were money handling breaches reported by subscribers in all size categories, two Category A subscribers accounted for 35% of the total.

One of these Category A subscribers self-reported 72 breaches. Examples included:

- an occasion where a branch staff member mistakenly suspended a client's account when the client attended the branch to pay for their policy (the staff member was subsequently given training in the correct processes).
- funds remaining in a trust account when they should have been moved into unclaimed monies (the subscriber reviewed its policies and procedures and instructed its account managers to redirect unclaimed monies to government treasury).

¹⁵ 5% in 2017 and 2018, 7% in 2019 and 11% in 2020.

A third example from the same subscriber involved an authorised representative failing to deposit cash and cheque payments into the correct trust account. The subscriber instructed the authorised representative to stop advising clients to pay their own accounts and provided training in the correct processes and procedures. The subscriber also advised the representative to deposit all cash and cheque payments within 24 hours and issued a reminder for the representative to meet its contractual obligations to the subscriber.

The second high-reporting Category A subscriber reported 58 breaches of Service Standard 7, although it transpired during the ACS verification conference that these were in fact four separate incidents that impacted 58 clients. The breaches occurred when the subscriber failed to provide clients with a refund of their premium within seven days. Because of a processing error, the subscriber did not have some clients' bank account details on file and had to post cheques instead of refunding the premiums via electronic funds transfer (EFT). This delayed the process and was further exacerbated by postal delays in some states due to COVID-19 lockdowns. The subscriber has since taken steps to ensure that when a client requests a refund, the client's bank account details must be entered into the system before the refund can be issued.

A Category E subscriber also reported a high number of breaches (15) caused by a failure to provide clients with their premium refund within seven days. As with the Category A subscriber above, clients' bank account details were not on file, which meant that the refunds could not be processed in a timely manner.

One Category D subscriber described an incident that accounted for 21 of the 23 money-related breaches it self-reported in 2020. The incident, which impacted 21 clients, had a number of causes, including delays in processing refunds, automatic renewal without the client's consent, and charging premium funding without the client's consent. These were due to the actions of one broker, who received training and supervision but was ultimately dismissed from employment. The subscriber financially reimbursed all impacted clients.

Service Standard 8: Training staff and authorised representatives

Under Service Standard 8 of the Code, subscribers are required to ensure that their staff and authorised representatives are competent and adequately trained, and their performance appropriately assessed and monitored.

There were 110 training-related breaches self-reported by 29 Code subscribers, making this the sixth most breached Service Standard in 2020. Eight of these (24%) were subscribers from Category C, while five (14%) were subscribers from Category A.

Between them, subscribers in Categories A and E accounted for just over 86% of all the training breaches, with Category A subscribers self-reporting a total of 52 breaches and Category E subscribers self-reporting 43.

One Category A subscriber was responsible for 21 training-related breaches – the highest number reported by any subscriber in 2020. The subscriber explained that the breaches came about as a result of too many client files being allocated to brokers, resulting in 20 separate breaches of the same nature across multiple branches. To remedy the matter and improve performance, the subscriber has implemented a client review process.

Another Category A subscriber self-reported 18 Service Standard 8 breaches, most of which were identified following incidents caused by human error. One example included the subscriber's authorised representative failing to verify calculation errors made by the premium funder. The

subscriber has put in place an ongoing training program for its staff and authorised representative to ensure this does not occur in the future.

Issues associated with acquiring another broker resulted in one Category E subscriber self-reporting 16 breaches of Service Standard 8. The subscriber explained that the staff members from the acquired business had not been sufficiently trained or authorised to provide advice to clients, leading to errors including failing to provide insurance schedules and statutory information, and failing to provide clients with 14 days' notice prior to the renewal of their policies. The subscriber has responded by re-training the relevant staff as broker assistants.

Service Standard 9: Responding to disasters

Service Standard 9 requires subscribers to respond to catastrophes and disasters in a timely, professional, practical and compassionate manner in conjunction with any industry-wide response. Surprisingly, given we saw a global pandemic and several natural disasters such as bushfires and floods in 2020, not a single subscriber recorded a breach of Service Standard 9.

Service Standard 10: Dispute resolution

Under Service Standard 10, subscribers must have an internal complaints and disputes handling process that meets the Code Complaints and Dispute process standards. In 2020, 12 subscribers reported 14 breaches of this Code standard, with all but one subscriber reporting a single breach.

Subscribers in Category E were the most widely represented, with seven subscribers reporting a breach. There were two subscribers in each of Categories A and B to report a breach and one in Category C. One of the Category A subscribers reported three breaches of Service Standard 10.

Almost all the breaches were caused by subscribers failing to meet the timeframes for acknowledging and/or responding to a client's complaint, as set out in the Code Complaints and Dispute process standards.

In some cases, systemic issues were to blame. One Category A subscriber reported that the client's complaint had not been registered in the internal dispute resolution (IDR) system and was therefore not acknowledged in accordance with the subscriber's IDR process. A Category D subscriber discovered via an internal audit that it was in breach of Service Standard 10, as its invoice template still referenced the Financial Ombudsman Service (FOS) instead of the Australian Financial Complaints Authority (AFCA).¹⁶ The breach was found to have impacted 7,000 clients, and the subscriber immediately updated all templates to include the correct information.

In other cases, breaches were the result of human error. A Category A subscriber breached Service Standard 10 when one of its brokers neglected to advise a client that the insurer required certain information from the client before being able to reinstate the client's motor vehicle policy. The client was subsequently involved in an accident, at which point they discovered that their policy renewal had not been processed and they had no cover.

The same subscriber reported another breach when a client complained about both a claim and the subscriber's IDR process after having issues contacting the claims representative. The claim was eventually settled, and the client was awarded an ex-gratia payment. The subscriber revised the claims process with the distributor to ensure that communication with clients and the timeliness of claims processing were improved.

¹⁶ AFCA replaced FOS on 1 November 2018.

Service Standard 11: Promoting the Code

Service Standard 11 obliges subscribers to promote the Code and to ensure that clients understand that they have the right to make a complaint under the Code. This is usually done by providing information about the Code in documentation to clients such as an FSG or PDS, and on the subscriber's website.

In 2020, there were 13 breaches of Service Standard 11 reported by four Code subscribers – two from Category C and two from Category E. The two Category E subscribers each reported five instances of non-compliance. One explained to the Compliance Manager that the breaches were identified via an external compliance audit which found that the subscriber had been providing clients with an old FSG that contained out-of-date information about the Code. While the subscriber had a more up-to-date version of the FSG containing the correct information, it had not been uploaded into the subscriber's system, resulting in 200 clients being sent the old version. The subscriber has since migrated its system to a new operating platform and clients are now receiving the correct FSG.

One Category C subscriber reported two breaches after identifying that information about the Code and the subscriber's complaints process was not published on its website. The breaches were discovered when the subscriber conducted a review of the website for the ACS. To remediate the breaches, the subscriber has redesigned its website to include the missing information, as well as ensuring that information about the Code and the complaints process is included in marketing procedures and checklists.

As part of the ACS Verification Program, the Compliance Manager conducts an audit of all subscribers' websites to ensure that information about the Code and the complaints process is published there. Individual subscribers have received feedback about how they can improve the promotion of the Code and their complaints process on their website.

Service Standard 12: Professionalism

Service Standard 12 is designed to ensure subscribers do not engage in any activity or inactivity that is reasonably likely to bring the insurance broking profession into disrepute. Breaches of this standard accounted for just over 5% of all self-reported Code breaches, making it the fourth most breached Code standard for 2020.

In all, 33 subscribers reported 174 professionalism-related breaches. While subscribers across all size categories reported at least one breach, those in Category E represented almost half of all subscribers to report a Service Standard 12 breach.

Almost a third (29%) of the breaches were reported by two subscribers – one Category A subscriber that reported 23 breaches and one Category D subscriber that reported 28 breaches.

Some of the breach examples provided by the Category D subscriber included:

- not matching the legal name in the brokering system to the legal entity name
- failing to send letters to clients, and
- emailing a client's information to a third party.

The subscriber explained that all 28 breaches, which were identified through file audits, were the result of human error – namely, staff failing to follow the correct processes and procedures.

Human error was also the cause of many of the 23 breaches reported by the Category A subscriber. Examples included several instances of staff failing to follow the instructions of either

the client or the insurer – the latter of which resulted in a client’s cover being cancelled due to non-payment. To address this, the subscriber has implemented internal training modules and discussions about professionalism-related breaches with its brokers as a ‘whole staff lesson’.

Other subscribers that were interviewed as part of the ACS Verification Program spoke of breaches that occurred due to brokers failing to send information to clients within the correct timeframe (for example, failing to send out a statement of advice, or not sending renewal notices within 14 days¹⁷), failing to renew a client’s policy or let them know that the policy had been cancelled, or accidentally sending one client’s information to another client.

Service Standard 12 is not a ‘data dump’ breach category

It is important to note that the Committee does not consider any of the abovementioned breach examples to be breaches of the Code’s professionalism standard. All should have been recorded as a breach of a different Code standard, such as Service Standard 1 (complying with the law) or Service Standard 5 (buying insurance).

We have consistently reminded subscribers to look more closely at how they categorise their breaches to ensure they are being recorded correctly. Service Standard 12 should not be viewed as a ‘data dump’ category for breaches that the subscriber is unsure how to classify because they have not taken the time to review the Code and determine the applicable standard.

¹⁷ As outlined on page 15, the Code does not require subscribers to provide renewal notices within a specified timeframe.

The root causes and impact of breaches

People-related issues were the root cause of most breaches

Subscribers named manual error and a failure to follow processes and procedures as the two main reasons for Code breaches in 2020.¹⁸ There were 650 breach incidents where manual error was identified as the root cause, and another 374 breach incidents where the root cause was given as process and procedure not being followed.

As in previous years, these two issues caused non-compliance across almost all Service Standards but most often in the areas of buying insurance (Service Standard 5.1) and legal compliance (Service Standard 1).

For breaches relating to buying insurance, subscribers cited manual error as the root cause of 325 incidents, while a failure to follow processes and procedures was given as the root cause of 143 incidents. For breaches of the Code's legal standards, manual error was provided as the root cause of 158 incidents. Processes and procedures not being followed was the root cause of 89 incidents related to legal compliance.

Subscribers also recorded a high number of incidents where the root cause was given as 'other'. In all, there were 300 such incidents, including 213 related to buying insurance and 25 for claims handling.

One Category C subscriber selected manual error as the root cause of most of its 59 self-reported breaches. According to the subscriber, the underlying reason was a high rate of staff turnover – in 2020, around 50% of staff at the organisation were new and inexperienced.

A Category D subscriber also named manual error as the root cause of the three privacy breaches it self-reported, after one of its brokers inadvertently sent emails to the wrong clients. The subscriber explained that it regularly tracks its brokers to identify any manual errors and provide appropriate training to prevent a recurrence. It also holds monthly one-on-one sessions with all brokers to address any issues as they arise. In the case of the three privacy breaches, the subscriber provided the broker with additional privacy training, which was subsequently rolled out to the wider broking team.

One Category A subscriber attributed a large proportion of its 111 self-reported breaches to a failure by staff to follow process and procedure. The subscriber explained during its ACS verification conference that it acquired several smaller broking firms in 2019, resulting in more than 100 new brokers coming on board. When the subscriber conducted reviews of each new broker's files, it identified several instances where existing processes and procedures had not been followed, along with a number of training gaps.

Good practice example

During its 2020 ACS verification conference, one Category A subscriber explained that it had improved its processes for identifying and addressing the root causes of incidents after taking on board feedback that was provided during a previous ACS verification conference.

The subscriber subsequently updated its Incident Register to ensure that both short-term and long-term remedial action is recorded for each incident. This improvement has enabled the subscriber to review all incidents so that root causes are clearly identified and addressed, and further incidents are prevented.

¹⁸ See Appendix E, Table 16.

The subscriber implemented basic training for all brokers, with refresher training conducted 18 months later, and created an employee handbook outlining the processes and procedures that all brokers must follow. This handbook is accessible to all brokers and is also used as a key training resource.

Code breaches impacted almost 21,000 clients

As part of their breach reporting, subscribers were asked to provide the number of clients that were impacted by the breach or breaches, as well as the total dollar financial impact of the breach on the client. Overall, 20,740 clients were reported as having been impacted by Code breaches, with a total financial impact (pre-remediation) of just under \$652,000.¹⁹

Self-reported breaches of Service Standard 5 of the Code resulted in the highest financial impacts to clients. A failure to provide adequate claims handling services resulted in 106 clients being financially impacted to the tune of \$307,861, while a failure to provide adequate insurance broking services resulted in a financial impact of \$294,618 to 3,095 clients.

One Category A subscriber reported a breach of the Code's buying insurance standard that resulted in a financial impact of \$85,000. The incident came to light when management of a client's file was transferred from one broker to another. The new broker did not explain to the client that their policy had been cancelled and that they were therefore uninsured. The client was only made aware of this when they attempted to make a claim on the policy. The matter was handled internally by the subscriber's litigation department, and a discussion was held with the affected branch to address issues relating to renewal disclosure and managing client expectations during the handover process from one broker to another.

Breaches of Service Standard 1 (legal obligations) affected 7,425 clients and had a financial impact of \$21,697. A Category A subscriber self-reported a breach of the Code's legal standards which, although it had no financial impact, affected 1,716 clients. The breach occurred when a cyber-attack caused a broker to click on a link in an email, which then forwarded a phishing email to a number of third parties, including several clients.

A single breach of Service Standard 10 (dispute resolution) – caused by a Category D subscriber's invoice template not having been updated to reflect the name change from FOS to AFCA – resulted in just over 7,000 clients being impacted. Surprisingly, there was no financial impact as a result of the breach.

Interpreting financial impact

The ACS Verification Program highlighted several instances where Code subscribers had misunderstood the definition of 'financial impact' in relation to breaches. In asking for the total financial impact of each breach, the Committee expects subscribers to provide figures based on the financial impact to clients before any remediation.

This means that if an ex-gratia payment is made to a client, we would expect to see the payment amount reflected in the financial impact column of the Breach Data Report. Similarly, any non-financial losses, reimbursements of fees/charges, or amounts awarded following an AFCA Determination are considered financial impacts and should be included in the Breach Data Report.

¹⁹ See Appendix E, Table 17.

Conversely, subscribers should not incorporate the amount claimed by the insured when reporting the total financial impact. The ACS Verification Program highlighted two instances of subscribers incorrectly including the amount claimed by clients into their financial impact reporting:

- A Category E subscriber reported a total financial impact of \$150,000 against a breach of the Code's claims handling standard. The breach involved a roof vandalism claim that was denied after a builder's report found that the damage was caused by wear and tear. During its ACS verification conference, the subscriber explained that \$150,000 was the amount claimed by the client rather than the total financial impact to the business.
- A Category C subscriber reported that a client complaint regarding non-disclosure of information when a claim was made resulted in a total financial impact of \$80,000. During its ACS verification conference, the subscriber clarified that it had reported the amount the client was claiming, and not the total financial impact to the business.

Complaints data key findings

In 2020, we saw the number of self-reported complaints rise sharply to 1,778 (up from 1,292 in 2019). Around a quarter of these complaints (26%) constituted a breach of the Code.

Despite this rise, we did not see a corresponding increase in the number of Code subscribers self-reporting a complaint. Instead, we saw our self-reporting complaints culture decline slightly, with 52% of Code subscribers self-reporting complaints in 2020 compared to 60% the previous year.²⁰ This result was significantly impacted by the influx of new subscribers to the 2020 ACS Program, making annual comparisons difficult.

One Category C subscriber interviewed for the ACS Verification Program reported 81% fewer complaints than the previous year (2 in 2020 compared to 11 in 2019). According to the subscriber, because staff were mostly working from home due to the pandemic, there were fewer opportunities for management to remind staff about how to identify and report complaints.

There were 208 Code subscribers (48% of the total) to self-report nil complaints in 2020, including one Category A subscriber and two Category B subscribers. There were also 190 subscribers in the smallest size category that did not report a single complaint that was handled via their IDR process.²¹

Two Category E subscribers that reported nil complaints in 2020 were interviewed for the ACS Verification Program. One explained that its brokers speak regularly with their clients to identify, discuss and resolve any issues before they become complaints. During these discussions, clients are made aware of the subscriber's IDR process and provided with the opportunity to make a complaint if they wish to do so.

Committee reminder

*Subscribers must record **all complaints that involve a Code breach in the Breach Data Report.***

The other Category E subscriber has never reported a complaint as part of its ACS and this was queried during the ACS verification conference. The subscriber explained that if a client phones to complain about an issue, and the issue is resolved immediately to the client's satisfaction, the subscriber does not record this as a complaint. The subscriber also said it did not believe that any of the complaints it has received from clients have been serious enough to record and report to the Committee.

Top products involved in complaints

In previous years, we have seen consistently high numbers of subscribers failing to specify the insurance product involved in a complaint, categorising the complaint instead as relating to 'other' products. To address this, the Committee included additional product categories in the 2020 ACS. While this has improved the consistency, accuracy and transparency of complaints data, it has also meant that comparisons with previous years' complaints reporting are not always feasible.

In 2020, there were complaints relating to all insurance products except extended warranty insurance.²² Motor vehicle insurance products were at the centre of most complaints (16%), with commercial motor vehicle insurance representing 9% of complaints and personal motor vehicle

²⁰ See Appendix F, Table 18.

²¹ See Appendix F, Table 19.

²² See Appendix F, Chart 15.

insurance representing 7%. In 2019, complaints about motor vehicle insurance were the subject of 18% of complaints.

Just under 14% of self-reported complaints were about small business insurance policies, down from 24% in 2019. A further 9% of complaints were recorded as relating to service rather than any specific product – a new category introduced in the 2020 ACS. Clarifying why ‘no product’ was recorded against 28 of its self-reported complaints, one Category A subscriber said that in some cases the complaint concerned an issue with the claims assessor, or a policy extension not being available, or the lack of coverage by the insurer.

Other newly introduced product categories for self-reported complaints were domestic insurance and landlord policies, which each accounted for around 5% of complaints in 2020.

Complaints about professional indemnity insurance increased slightly, from 4% in 2019 to just over 5% in 2020. Complaints relating to home building policies and residential strata title insurance both fell by around 3%, with around 5% of all complaints relating to home building insurance and just over 4% relating to residential strata title insurance.

Top issues involved in complaints

Since 2015, service has been the most complained about issue and 2020 was no different. The top issue (43%) of all self-reported complaints related to service levels, including complaints about the level of service clients received when making a claim (26%) and complaints relating to service in general (17%).²³

While there was no change to the percentage of complaints relating to general service, complaints relating to claims service fell in 2020 – down from 36% in 2019. Subscribers in Categories A and E self-reported the highest number of these complaints, together accounting for almost two-thirds of the total.

One Category D subscriber self-reported 18 complaints related to claims service. The complaints related to a particular online caravan hire platform through which the subscriber was selling insurance as an authorised representative, via a binder agreement, on behalf of the insurer.

The remaining issues of complaints were spread across several other areas. Complaints about instructions (4%), charges (4%), advice (3%) and other non-identified issues (6%) all fell in 2020. Several new issues were included as options in the ACS, including complaints about cover (11%), pricing (8%) and premium funding (4%).

Top outcomes involved in complaints

The majority of self-reported complaints were resolved by subscribers issuing an apology, explanation and/or acknowledgement of the complaint.²⁴

The number of complaints resolved in favour of the client fell to 18% in 2020, down from 27% in 2019. The number of complaints resolved in the insurance broker’s favour also fell, from 11% in 2019 down to 8% in 2020.

Complaints resolved by mutual agreement dropped from 17% in 2019 to 7% in 2020. A further 6% of complaints were either withdrawn by the client or not actioned because the client did not respond, while 4% of complaints were resolved after the client took their business elsewhere.

²³ See Appendix F, Chart 16.

²⁴ See Appendix F, Chart 17.

A new category, introduced in the 2020 ACS, reflected that 14% of complaints were identified as complaints against the insurer.

Complaint resolution timeframes

Complaints resolved within 21 days

The Committee was pleased to note a significant improvement in complaints handling timeframes in 2020, ²⁵ with 68% of complaints resolved within 21 days compared to 59% in 2019. Between them, 186 insurance brokers (44% of all Code subscribers) self-reported a total of 1,202 complaints that were resolved within 21 days. One Category E subscriber self-reported 66 complaints as resolved within this timeframe – the most out of any subscriber.

The improvement in performance on this measure follows on from the guidance provided in our 2019 Own Motion Inquiry (OMI) report, [Improving Complaints Handling Timeframes](#).²⁶ It is gratifying to note that Code subscribers have considered the recommendations set out in the OMI and taken steps to put them into practice.

Pleasingly, it also indicates that most Code subscribers had prepared well in advance for ASIC's [Regulatory Guide 271 Internal Dispute Resolution](#)²⁷ (RG271), which came into effect on 5 October 2021. RG271 sets new standards and requirements for complaints handling across the financial services sector, including the requirement to resolve standard complaints within 30 calendar days instead of 45 calendar days. With subscribers resolving more than two-thirds of all complaints in 2020 well within 30 calendar days, the Committee is confident that insurance brokers are well placed to meet their obligations under RG271.

Complaints resolved between 21 and 45 days

Seventy-four Code subscribers reported having resolved a total of 255 complaints (14%) between 21 days and 45 days after the complaint was lodged. A third of these complaints were self-reported by Category A subscribers.

Complaints resolved beyond 45 days

Between them, 64 Code subscribers self-reported 167 complaints (9% of the total) that took more than 45 days to resolve. Just under half (44%) of these complaints were self-reported by Category A subscribers.

Some of the reasons given for complaints not being resolved within 45 days included the complexity of the matter, the client and/or the insurer not providing adequate information in time, the matter being referred to AFCA, and the insurer delaying their decision.

One Category A subscriber said some complaints were not resolved within 45 days because staff were unable to access hardcopy files relating to the complaints, as they were located in the office which was closed due to COVID-19 lockdowns. Several subscribers pointed to delays by the complainant in responding to queries. One Category E subscriber was unable to resolve the complaint within 45 days because the client failed to respond to the subscriber's email queries. Similarly, a Category D subscriber was delayed in resolving the complaint because it was waiting on information from both the client and a third party in order to settle a claim.

²⁵ See Appendix F, Chart 18.

²⁶ See <https://insurancebrokerscode.com.au/app/uploads/2020/03/201910-IBCCC-OMI-IDR-timeframes-Oct-2019.pdf>.

²⁷ See <https://asic.gov.au/media/3v2oejls/rq271-published-30-july-2020-20210608.pdf>.

Subscriber readiness for ASIC RG271 Internal Dispute Resolution

Subscribers that participated in the 2020 ACS Verification Program were asked about their preparedness for the new IDR timeframes set out in RG271. Pleasingly, most said they had already implemented RG271 into their complaints handling systems and processes, and in the case of the new subscribers under the Steadfast umbrella group, each had been offered training on the new requirements. In addition to aligning its IDR process to RG271, a Category D subscriber has also created two manuals outlining the company's complaints procedures, with one of these manuals designed specifically for its brokers. Concerningly, one Category E subscriber said it was unaware of RG271. The Compliance Manager has subsequently provided the subscriber with guidance on the new ASIC IDR requirements, along with a reminder to comply with its obligations.

RG271 – recording and analysing complaints information

Compliance with RG271 is not just about meeting the established IDR timeframes. ASIC also includes directions relating to the collection, analysis and internal reporting of complaints data (see RG271.179–182). The Committee strongly supports these directions and urges Code subscribers to take note of the following ASIC requirements and recommendations for managing and using their complaints data.

Recording complaints data

Under RG271, financial services firms must have an effective system that records information about complaints, as well as tracking their progress. Complaint systems should be designed to suit the nature, scale and complexity of a firm's business, including the number of complaints it receives. (For example, firms that receive few complaints might use a spreadsheet to record complaints information, while firms with large volumes of complaints are expected to use specialised complaints software or to integrate complaint management data fields into existing customer relationship management systems.)

Analysing complaints data

RG271 also emphasises the need for firms to review and analyse their complaints data on a regular basis. This includes data on:

- the number of complaints received and closed
- the nature of complaints (e.g. problem and product involved)
- the time taken to acknowledge and resolve complaints
- the outcome of complaints
- possible systemic issues identified, and
- the number of complaints escalated to AFCA.

By analysing this information, firms are able to monitor the performance of their IDR process, identify possible systemic issues and areas where improvements are required, and identify matters that are likely to need to be reported to ASIC under the Corporations Act.

Code compliance and monitoring activities

Improving processes and procedures to enhance Code compliance

During their ACS verification conferences, participating subscribers provided examples of how they have actively improved particular processes and procedures during the year to ensure compliance with the Code.²⁸ For some, this involved a fresh approach to the way they manage renewals, while for others, the focus was on improving communications with the client, as well as enhancing the overall client experience.

At the larger end of the spectrum, one Category B subscriber has developed a portal where clients can upload all relevant information when making a claim. The portal has improved efficiencies by enabling brokers to see at a glance whether any information is missing from the claim and follow it up with the client. It has also simplified the overall claims reporting process. The subscriber makes regular improvements to the portal based on feedback from clients and insurers.

Another Category B subscriber reported a similar initiative, where clients lodge claims online using standardised forms. According to the subscriber, automating the claims process has made it easier for clients and improved their overall experience, while the insurer – who provided guidance on the creation of the online forms – is also satisfied, as the subscriber’s new online claims lodgment process reflects its own.

To stay on top of renewals, one Category D subscriber has implemented a process whereby its brokers are advised at the start of each week about any upcoming renewals, including those that are due to expire over the following weekend. This allows the brokers to ensure that all renewals are addressed during the working week and no clients will be left uninsured if their renewal expires on a Saturday or Sunday. Management supports this process by sending out monthly reports to keep brokers informed about forthcoming renewals.

Two Category E subscribers also provided good-practice examples of improvements to their renewal process. One conducted an internal review of its policies and procedures related to personal accident and illness insurance. As part of the review, the subscriber actively sought feedback and suggestions from its own team, as well as the Steadfast parent company. By doing this, the subscriber believes it has created a positive organisational culture where staff feel they have played a key role in improving processes.

The other Category E subscriber has introduced an electronic renewal spreadsheet – an interactive document that sits on the company’s intranet. Staff are able to update the spreadsheet by adding comments and dates, whilst a designated administrator is responsible for running weekly reports, reviewing the data to ensure that all renewals are up to date, and contacting relevant team members to action any outstanding items.

Responding to its different clients’ needs, one Category D subscriber has structured its business into two units – one that caters to consumer clients and one that focuses on business clients. According to the subscriber, this has improved client communication and allowed brokers to tailor their services according to what the client wants (for example, giving a business client the option of a phone call or a face-to-face meeting to discuss a renewal).

One Category A subscriber updated its refund procedures and now only processes client refunds via EFT. The subscriber made this decision after New Zealand announced it was phasing out the

²⁸ See Appendix G, Table 21.

use of cheques. While cheques are still accepted in Australian banks, the subscriber recognised that most clients now use online banking and prefer to have their refunds processed via EFT, as the money is received immediately.

Monitoring websites to ensure Code compliance

Each year, the ACS questionnaire asks Code subscribers to state which compliance monitoring activities they have undertaken during the reporting period.²⁹ Included in the list of options are three relating to whether the subscriber monitors the information published on their website to ensure it includes information about the Code, the IDR process and the external dispute resolution (EDR) process.

By including information about the Code and the complaints process on their website, subscribers ensure they are complying with Service Standard 11 of the Code, which requires them to promote the Code and make clients aware that they have the right to make a complaint.

The Committee was disappointed to note that only 55% of subscribers said they undertook a compliance monitoring activity that involved checking whether their website includes information about the Code, whilst only 53% said they monitored whether their website includes information about their IDR and/or EDR process.³⁰

These results prompted the Compliance Manager to review the website of each subscriber that took part in the 2020 ACS Verification Program to determine any unidentified or unreported breaches of Service Standard 11. Based on the findings of these reviews, the Committee makes the following recommendations to all subscribers.

Recommendations for improving Code-related information on your website

- Ensure your website includes a separate page dedicated to the Insurance Brokers Code of Practice. Do not simply include a link to the Code itself from your home page or other non-specific page.
- Your web page about the Code should specify that you are a Code subscriber and include information about the Code's 12 Service Standards. This is a positive selling point for clients, as it demonstrates that you are dedicated to delivering them better outcomes.
- Check your FSG to ensure it contains up-to-date information and includes reference to your subscription to the Code.
- Ensure that both your website and FSG include information about a client's right to make a complaint, along with clear advice about your IDR and EDR processes so that clients understand how to make a complaint.
- Check that all information on your website and FSG is current (e.g. make sure the EDR process refers to AFCA, not FOS).

²⁹ See Appendix G, Table 21.

³⁰ Figures represent the percentage of Code subscribers who stated that they undertook a compliance monitoring activity in the particular area.

Conclusion

The ACS Verification Program is a vital component of the Committee's monitoring activities. It allows us to validate and interpret the data we receive from Code subscribers, and to have meaningful discussions about what they are doing well and areas for improvement. Importantly, the Program also provides us – and subscribers – with insight into where the industry sits in terms of breach reporting, Code compliance and best practice.

Overall, the participating subscribers have demonstrated a positive approach to their compliance monitoring and breach data reporting for the 2020 reporting period. As this report indicates, some Code subscribers need to examine their monitoring and reporting culture and processes to ensure they are identifying and capturing all Code breaches and complaints, while others should closely review how they interpret specific Code obligations to ensure they match the Committee's expectations.

The data and information contained in this report provide valuable insights into emerging issues on risk and compliance, along with recommendations from the Committee and examples of better practice from some of the Code subscribers that participated in the 2020 ACS Verification Program. We expect all Code-subscribing insurance brokers to consider implementing the recommendations and examples for their organisation.

Appendices

APPENDIX A: ABOUT THE CODE	36
The Code	36
Service Standards	36
Table 1: The 12 Service Standards.....	36
The Committee	37
Compliance Manager	37
APPENDIX B: CODE SUBSCRIBERS	38
Table 2: Categorisation of Code subscribers by size of business.....	38
Table 3: Number of Code subscribers by state (head office) and size of operation	38
Table 4: Number of branches (including head office) by state and size of operation ...	39
APPENDIX C: DATA TRENDS	40
Chart 1: Trends and relationships in breach and complaints data since 2015	40
Chart 2: Self-reporting culture in 2020	40
Table 5: Industry summary (all Code subscribers)	41
Chart 3: Top six categories of Code breaches self-reported since 2015	41
Data trend - Code subscribers Category A	42
Table 6: Sector summary (Category A).....	42
Chart 4: Top six categories of Code breaches self-reported since 2015 in Category A	42
.....	42
Data trend - Code subscribers in Category B	43
Table 7: Sector summary (Category B).....	43
Chart 5: Top six categories of Code breaches self-reported since 2015 in Category B	43
Data trend - Code subscribers in Category C	44
Table 8: Sector summary (Category C).....	44
Chart 6: Top six categories of Code breaches self-reported since 2015 in Category C	44
Data trend - Code subscribers in Category D	45
Table 9: Sector summary (Category D).....	45
Chart 7: Top six categories of Code breaches self-reported since 2015 in Category D	45
Data trend - Code subscribers in Category E	46
Table 10: Sector summary (Category E).....	46
Chart 8: Top six categories of Code breaches self-reported since 2015 in Category E	46
APPENDIX D: SELF-REPORTED BREACH DATA	47
Table 11: Number of Code subscribers (in % of total Code subscribers) self-reporting	47
Code breaches since 2015	47
Table 12: Number of self-reported Code breaches by size of Code subscriber in 2020	47
.....	47
Table 13: Analysis of high volumes of self-reported Code breaches in 2020.....	47
Table 14: Number of breach(es) by timeframe for immediate remedial action(s).....	49
Table 15: Number of breach(es) by timeframe for long term remedial action(s).....	49

APPENDIX E: ROOT CAUSE AND IMPACT OF SELF-REPORTED CODE BREACHES IN 2020	50
.....	
Table 16: Root causes of self-reported breaches by Code section in 2020	50
Chart 9: Financial impact to client(s) by root cause of self-reported breach(es)	51
Chart 10: Number of client(s) impacted by root cause of self-reported breach(es)	51
Chart 11: Number of self-reported breach(es) by root cause	51
Table 17: Impact of self-reported breaches by Code section in 2020	52
Chart 12: Financial impact to client(s) by Product/Service Types	53
Chart 13: Number of client(s) impacted by Product/Service Types	53
Chart 14: Number of self-reported breach(es) by Product/Service Type	53
APPENDIX F: SELF-REPORTED COMPLAINTS DATA	54
Table 18: Number of Code subscribers (in % of total Code subscribers) self-reporting complaints since 2015	54
Table 19: Number of self-reported complaints by size of Code subscriber in 2020	54
Chart 15: Top product categories of total self-reported complaints in 2020	54
Chart 16: Top issue categories of total self-reported complaints in 2020	55
Chart 17: Top outcome categories of total self-reported complaints in 2020	55
Chart 18: Resolution timeframe categories of self-reported complaints in 2020	55
Table 20: Analysis of high volumes of self-reported complaints in 2020	56
APPENDIX G: COMPLIANCE MONITORING ACTIVITIES IN 2020	59
Table 21: Compliance monitoring activities undertaken by Code subscribers	59

Appendix A: About the Code

The Code

The 2014 Insurance Brokers Code of Practice ([the Code](#)) sets standards of good industry practice for the insurance brokers that have agreed to follow its standards when dealing with current and prospective individual and small business clients. The Code is owned and published by the National Insurance Brokers Association ([NIBA](#)) and forms an important part of the broader national consumer protection framework and financial services regulatory system.

In September 2018, NIBA appointed Marigold Magnaye to undertake a review of the Code, which remains ongoing.

Service Standards

By subscribing to the Code, insurance brokers have committed to continuously improving standards of practice and service in their sector; promoting informed decision-making about their services; and acting fairly and reasonably in delivering those services.

The Code contains the following 12 Service Standards that apply to all insurance broking services delivered to individuals and small businesses by Code subscribers across Australia.

Table 1: The 12 Service Standards

1.	We will comply with all relevant law.
2.	We will transparently manage any conflicts of interest that may arise.
3.	We will clearly tell you if we do not act for you.
4.	We will clearly tell you about the scope of our covered services.
5.	We will discharge our duties diligently, competently, fairly and with honesty and integrity.
6.	We will clearly tell you how our covered services are paid for before we provide them and answer any questions you have.
7.	We will handle any money received in accordance with relevant law and any agreement with you.
8.	We will ensure that we and our representatives are competent and adequately trained to provide the relevant services and will maintain this competence.
9.	We will respond to catastrophes and disasters in a timely, professional, practical and compassionate manner in conjunction with any industry-wide response.
10.	We will ensure that we have an internal complaints and disputes handling process that meets the Code Complaints and Dispute process standards.
11.	We will support NIBA in promoting the Code and make information on the Code (including how to make a complaint) and our Covered Services readily available to you.
12.	We will not engage in activity or inactivity that is reasonably likely to bring the insurance broking profession into disrepute.

The Committee

The Insurance Brokers Code Compliance Committee ([the Committee](#)) is an independent compliance monitoring body established under section 3 of the Insurance Brokers Code Compliance Committee Charter and formally approved by NIBA on 5 September 2014.

The Committee comprises three members – an independent Chair, and Industry Representative and a Consumer Representative. The Committee also has alternate appointments for the Industry and Consumer Representative position to cater for situations where there might be a conflict of interest or an unavailability to attend meetings.

Compliance Manager

The Australian Financial Complaints Authority ([AFCA](#)) provides Code monitoring and administration services to the Committee and NIBA, by agreement. AFCA has appointed a dedicated team of staff (Compliance Manager) within its office to undertake that task.

Appendix B: Code subscribers

Table 2: Categorisation of Code subscribers by size of business

up to 2018 ACS		from 2019 ACS onwards	
large	over 100 FTE ³¹ staff	Category A	over 100 FTE staff
medium	31-100 FTE staff	Category B	51-100 FTE staff
		Category C	31-50 FTE staff
small	21-30 FTE staff	Category D	21-30 FTE staff
micro	0-20 FTE staff	Category E	0-20 FTE staff

Table 3: Number of Code subscribers by state (head office) and size of operation³²

As at 30 June 2021	ACT	NSW	NT	QLD	SA	TAS	VIC	WA	Total	In %
Category A	-	15	-	2	1	-	16	3	37	8%
Category B	-	9	-	1	-	1	6	5	22	5%
Category C	-	11	-	4	3	-	9	7	34	7%
Category D	-	9	-	9	1	1	9	3	32	7%
Category E	2	104	1	59	22	9	97	37	331	73%
Total	2	148	1	75	27	11	137	55	456³³	
In %	<1%	33%	<1%	16%	6%	2%	30%	12%		
<i>In comparison to 30/06/2020</i>	4	148	1	78	31	10	137	58	467 ³⁴	
<i>In comparison to 30/06/2019</i>	2	100	1	43	21	6	77	43	293	
<i>In comparison to 30/06/2018</i>	2	103	1	44	23	6	78	43	300	
<i>In comparison to 30/06/2017</i>	2	106	1	46	22	7	89	45	318	

A list of Code subscribers can be found at <https://insurancebrokerscode.com.au/about/about-the-code/code-subscriber-register/>.

³¹ FTE – full time equivalent.

³² Code subscribers are counted by Australian Financial Service Licence (AFSL).

³³ The decrease in the number of Code subscribers is due to mergers and acquisitions.

³⁴ The increase in the number of Code subscribers follows a decision made by Steadfast that all its members became Code subscribers effective 1 December 2019. For information about Code subscription please contact NIBA at niba@niba.com.au or telephone (02) 9964 9400.

Table 4: Number of branches (including head office) by state and size of operation

<i>As at 30 June 2021</i>	<i>ACT</i>	<i>NSW</i>	<i>NT</i>	<i>QLD</i>	<i>SA</i>	<i>TAS</i>	<i>VIC</i>	<i>WA</i>	<i>Total</i>	<i>In %</i>
Category A	21	366	17	262	88	13	273	133	1,173	59%
Category B	3	29	1	19	2	62	29	3	148	7%
Category C	1	43	1	25	4	-	48	23	145	7%
Category D	-	27	-	28	2	4	15	4	80	4%
Category E	6	155	1	86	29	11	122	42	452	23%
Total	31	620	20	420	125	90	487	205	1,998	
In %	2%	31%	1%	21%	6%	5%	24%	10%		

Overseas operations

- 10 Category A and 4 Category E companies noted that they also have operations overseas.
- This included being part of a global company, other companies within the international group having overseas operations or a completely separate entity operating overseas.

Appendix C: Data trends

Chart 1: Trends and relationships in breach and complaints data since 2015

Self-reported by all Code subscribers over the past six years to the Committee.

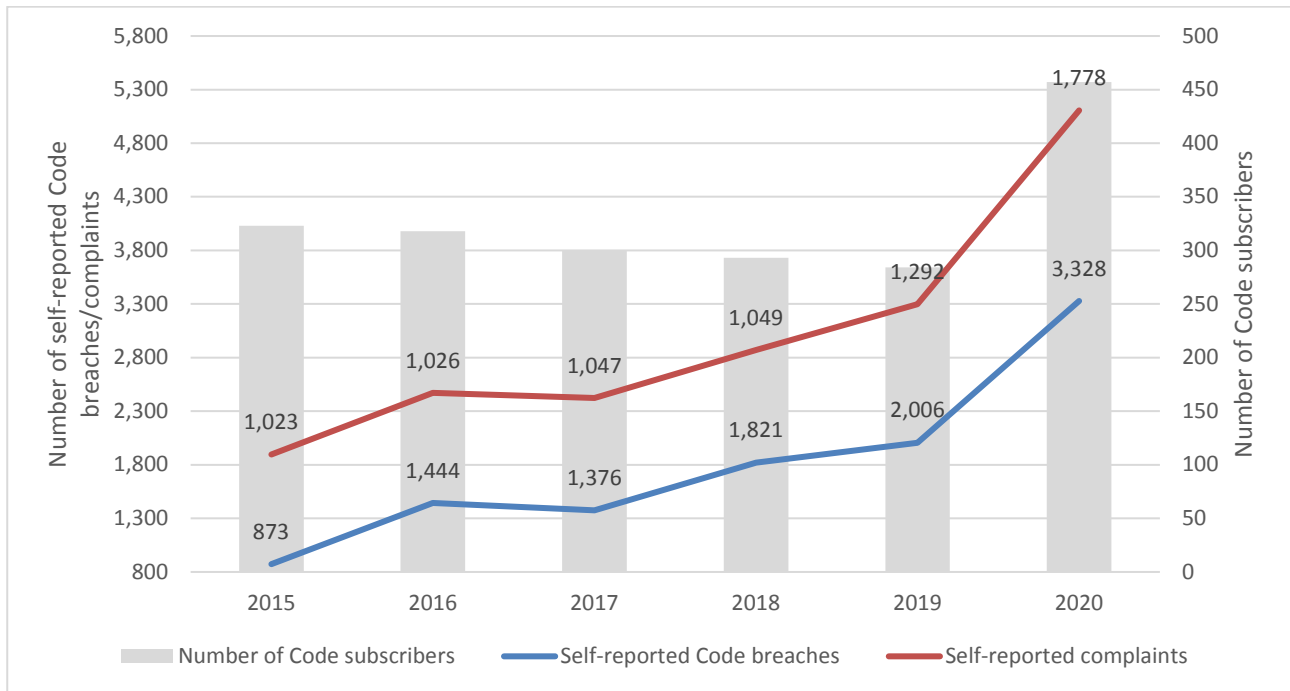


Chart 2: Self-reporting culture in 2020

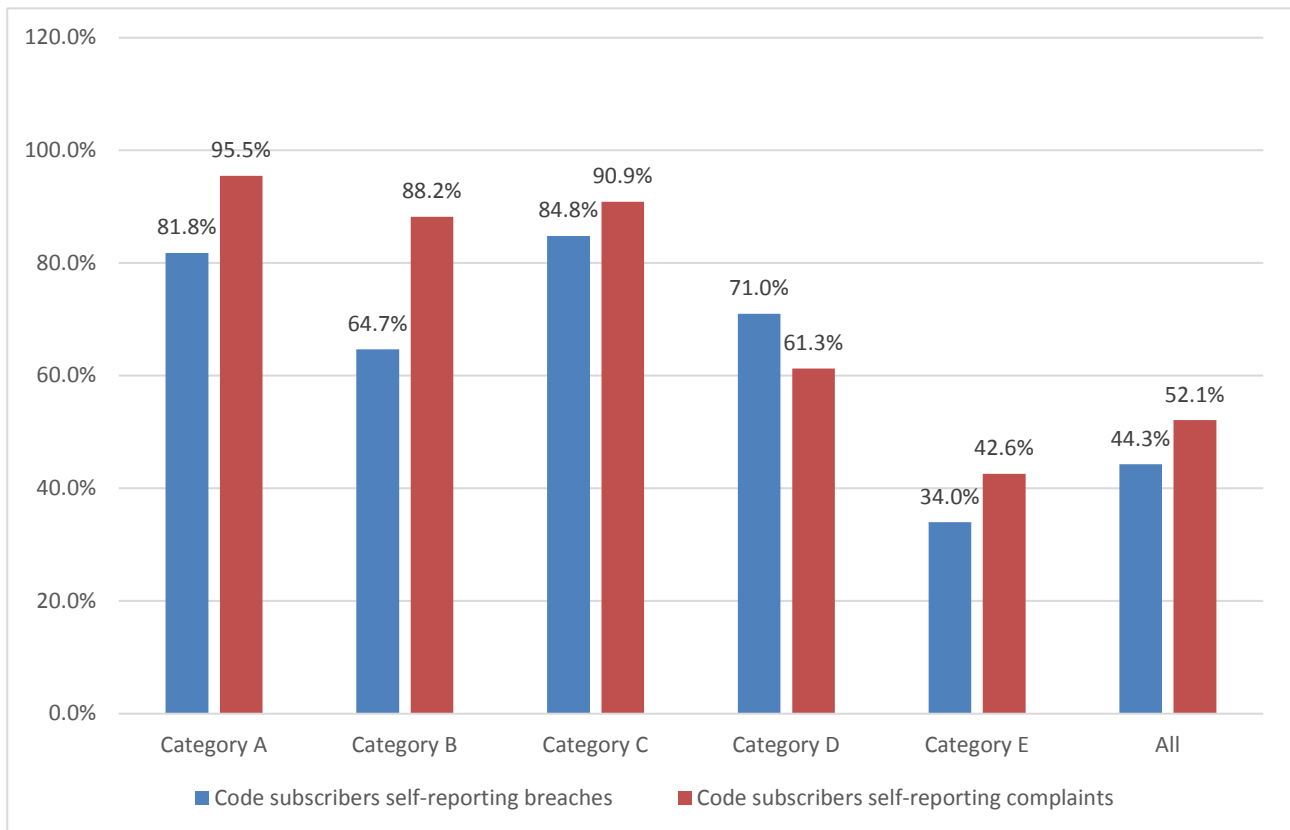
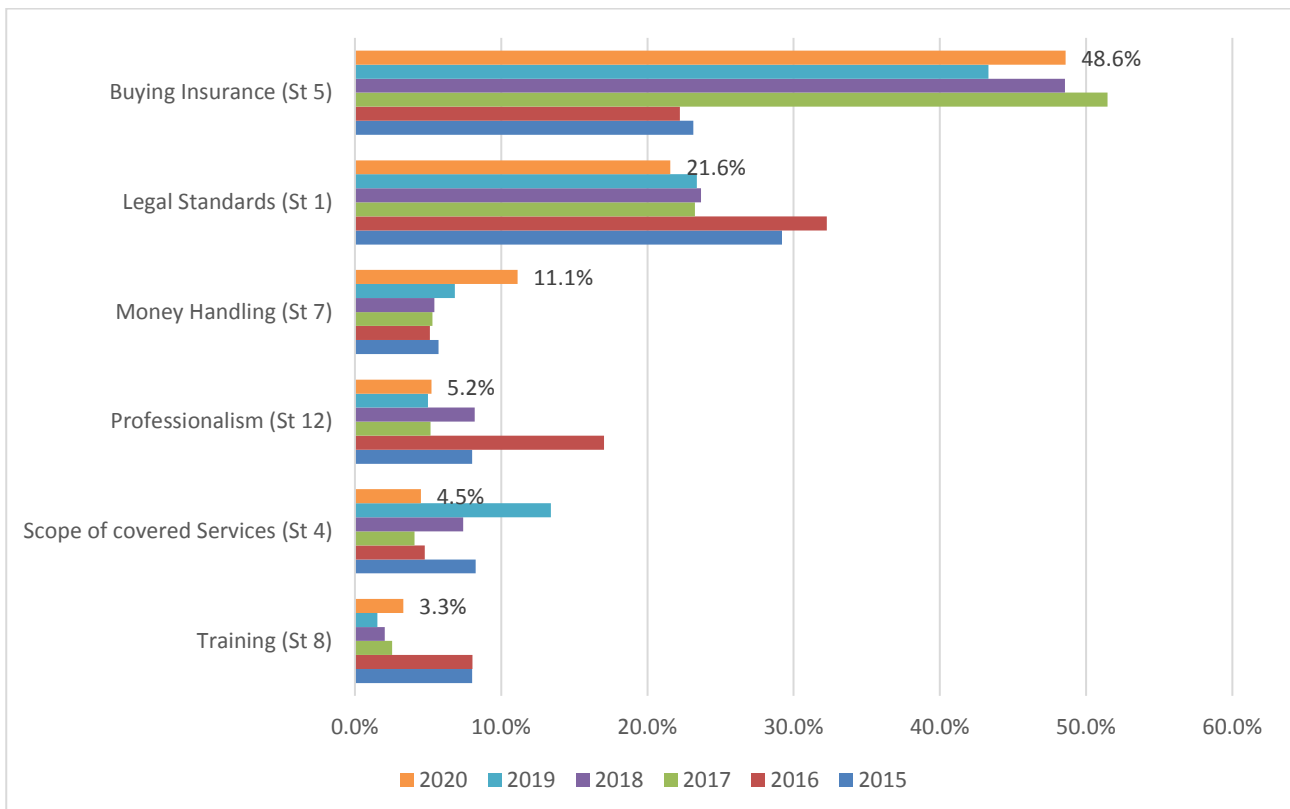


Table 5: Industry summary (all Code subscribers)

	2015	2016	2017	2018	2019	2020
Number of Code subscribers	323	318	300	293	284 ³⁵	457
Number of branches (including head office)	n/a	n/a	n/a	1,550	1,471	1,998
Total of self-reported Code breaches	873	1,444	1,376	1,821	2,006	3,328
Mean of self-reported Code breaches	2.7	4.4	4.7	6.2	7.1	7.8
% of Code subscribers self-reporting Code breaches	32%	42%	41%	43%	51%	44.3%
Total of self-reported complaints	1,023	1,026	1,047	1,049	1,292	1,778
Mean of self-reported complaints	3.2	3.2	3.6	3.6	4.5	4.1
% of Code subscribers self-reporting complaints	52%	54%	57%	61%	60%	52.1

Chart 3: Top six categories of Code breaches self-reported since 2015



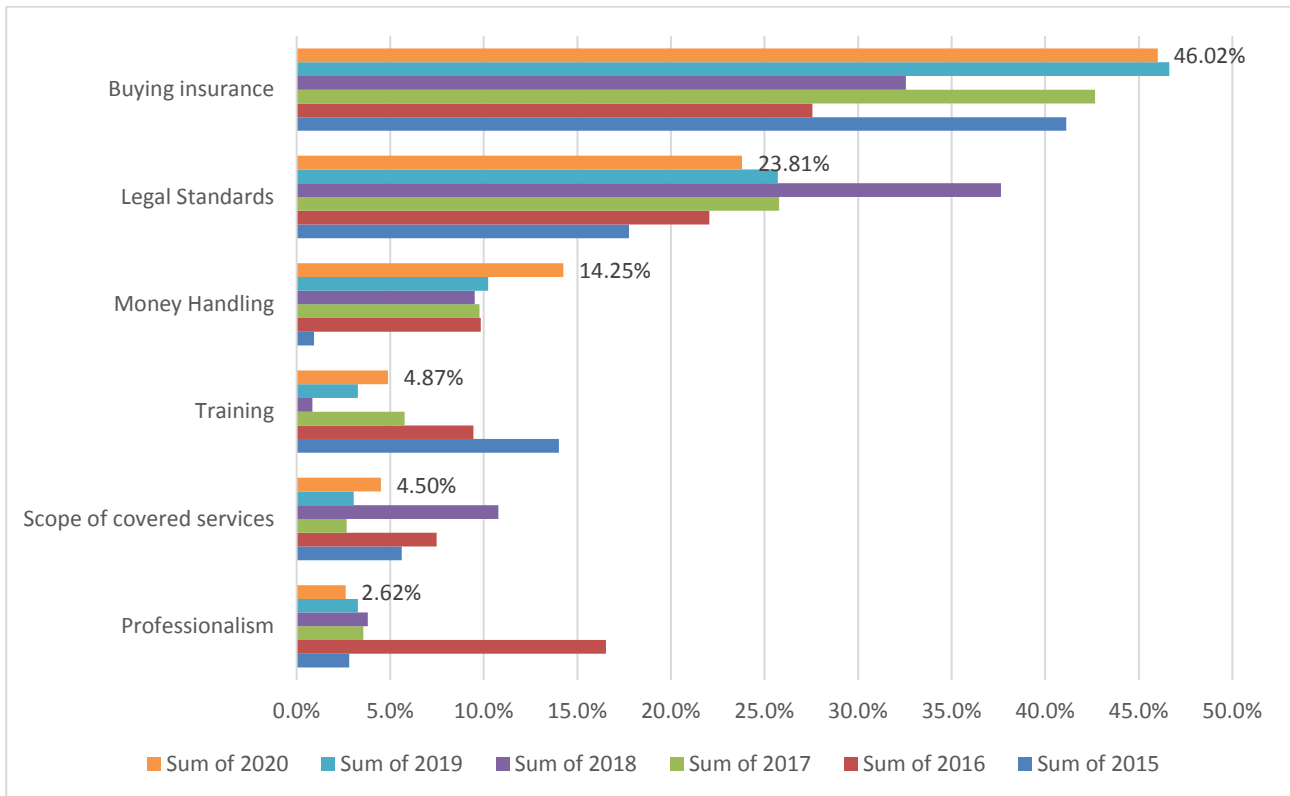
³⁵ Code subscribers are counted by Australian Financial Service Licence (AFSL), not counting the new Steadfast members who became Code subscribers effective 1 December 2019 and were not involved in the 2019 ACS Program. Some Code subscribers are represented by more than one AFSL.

Data trend - Code subscribers Category A

Table 6: Sector summary (Category A)

	2015	2016	2017	2018	2019	2020
Number of Code subscribers	13	25	21	26	29	37
Number of branches (including head office)	n/a	n/a	n/a	933	955	1,173
Total of self-reported Code breaches	44	302	190	397	454	1,067
Mean of self-reported Code breaches	8.8	11.7	10.8	15.3	15.7	48.5
% of Code subscribers self-reporting Code breaches	59%	52%	94%	72%	85%	81.8%
Total of self-reported complaints	52	311	410	300	554	522
Mean of self-reported complaints	14.2	12.4	24.1	11.5	19.1	23.7
% of Code subscribers self-reporting complaints	88%	68%	100%	94%	90%	95.5%

Chart 4: Top six categories of Code breaches self-reported since 2015 in Category A

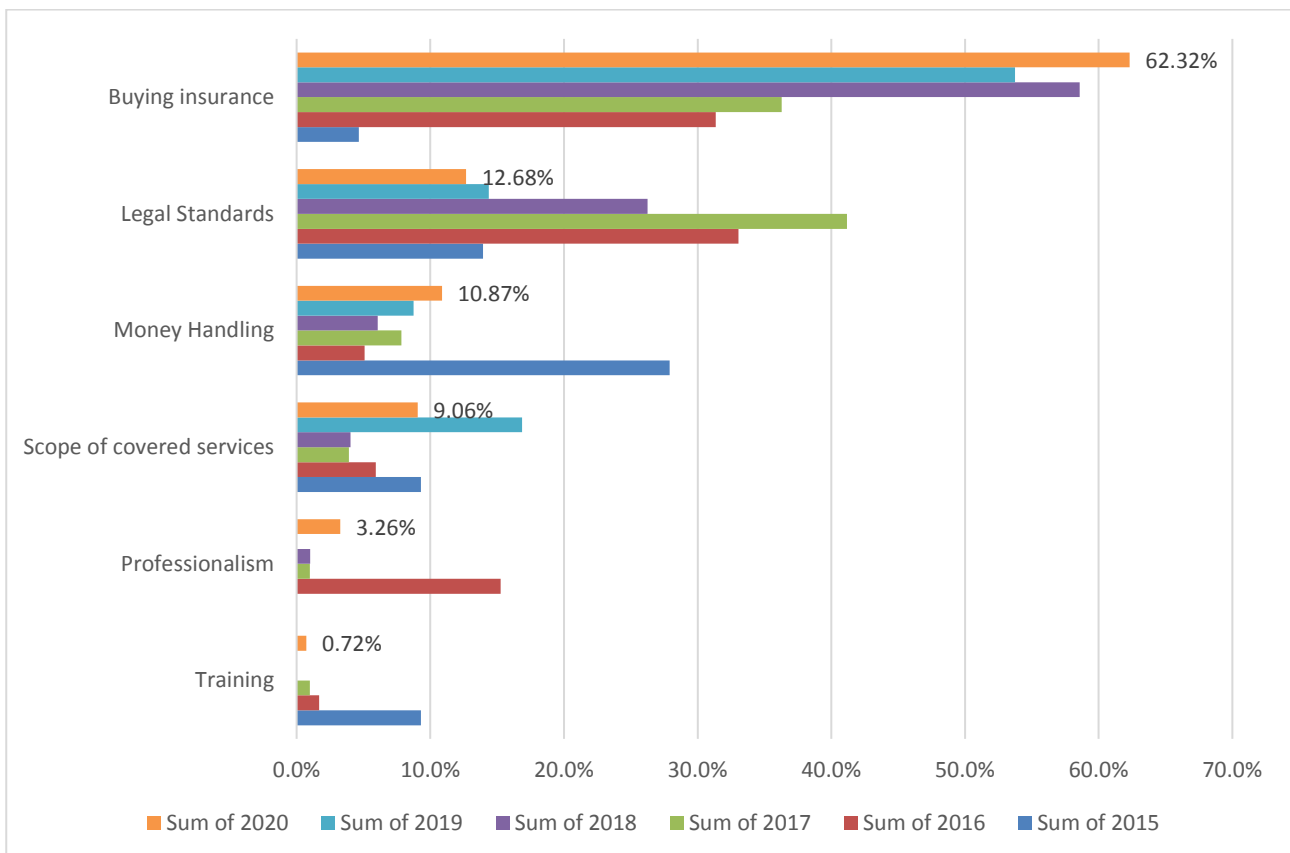


Data trend - Code subscribers in Category B

Table 7: Sector summary (Category B)

	2015	2016	2017	2018	2019	2020
	Cat B&C	Cat B&C	Cat B&C	Cat B&C	Cat B	Cat B
Number of Code subscribers	26	49	46	52	18	22
Number of branches (including head office)	n/a	n/a	n/a	240	76	148
Total of self-reported Code breaches	113	383	305	372	155	278
Mean of self-reported Code breaches	4.4	7.6	6.6	7.2	8.6	16.4
% of Code subscribers self-reporting Code breaches	50%	69%	50%	59%	64%	64.7%
Total of self-reported complaints	143	204	225	275	88	133
Mean of self-reported complaints	6.4	4.2	4.9	5.3	4.9	7.8
% of Code subscribers self-reporting complaints	83%	83%	91%	82%	86%	88.2%

Chart 5: Top six categories of Code breaches self-reported since 2015 in Category B

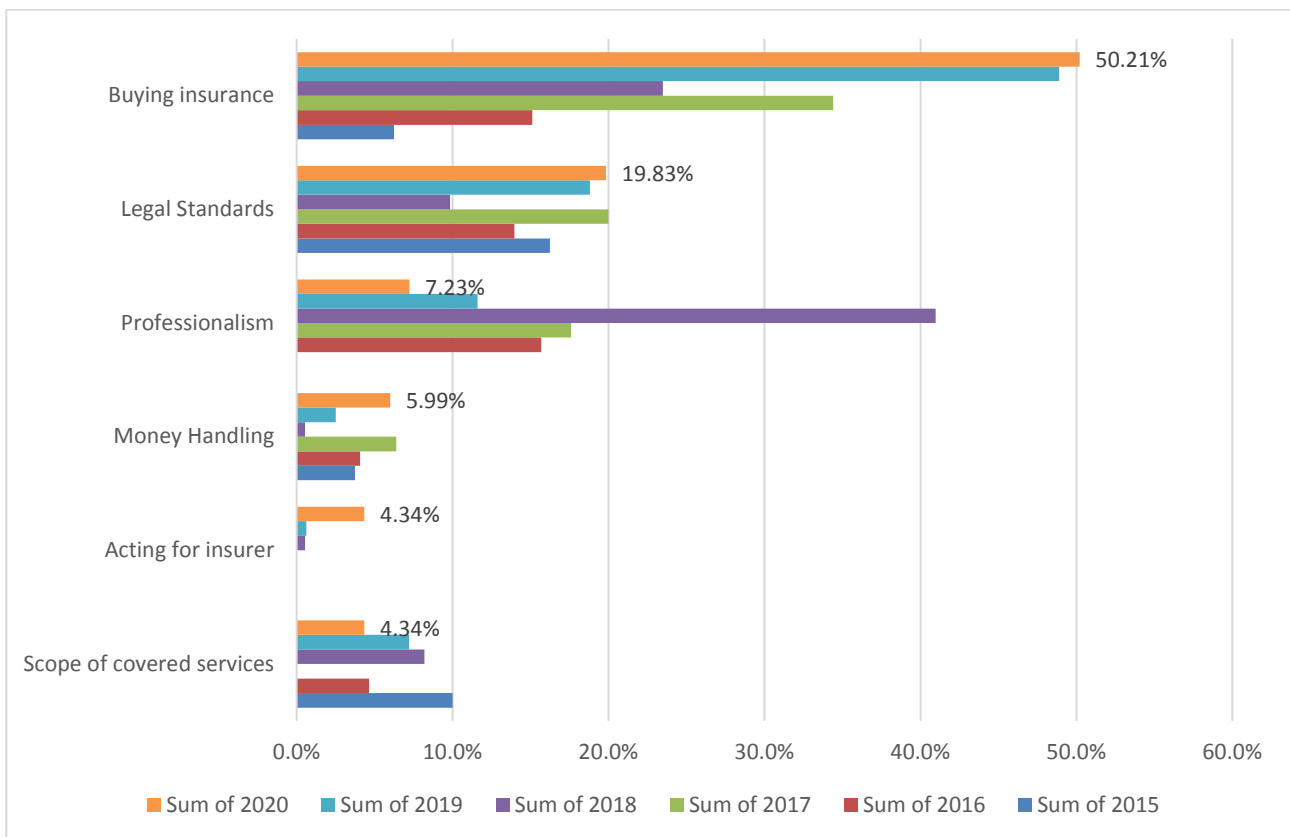


Data trend - Code subscribers in Category C

Table 8: Sector summary (Category C)

	2015	2016	2017	2018	2019	2020
	Cat B&C	Cat B&C	Cat B&C	Cat B&C	Cat C	Cat C
Number of Code subscribers	26	49	46	52	35	34
Number of branches (including head office)	n/a	n/a	n/a	240	170	145
Total of self-reported Code breaches	113	383	305	372	469	495
Mean of self-reported Code breaches	4.4	7.6	6.6	7.2	13.4	15.0
% of Code subscribers self-reporting Code breaches	50%	69%	50%	59%	74%	84.8%
Total of self-reported complaints	143	204	225	275	250	238
Mean of self-reported complaints	6.4	4.2	4.9	5.3	7.1	7.2
% of Code subscribers self-reporting complaints	83%	83%	91%	82%	91%	90.9%

Chart 6: Top six categories of Code breaches self-reported since 2015 in Category C

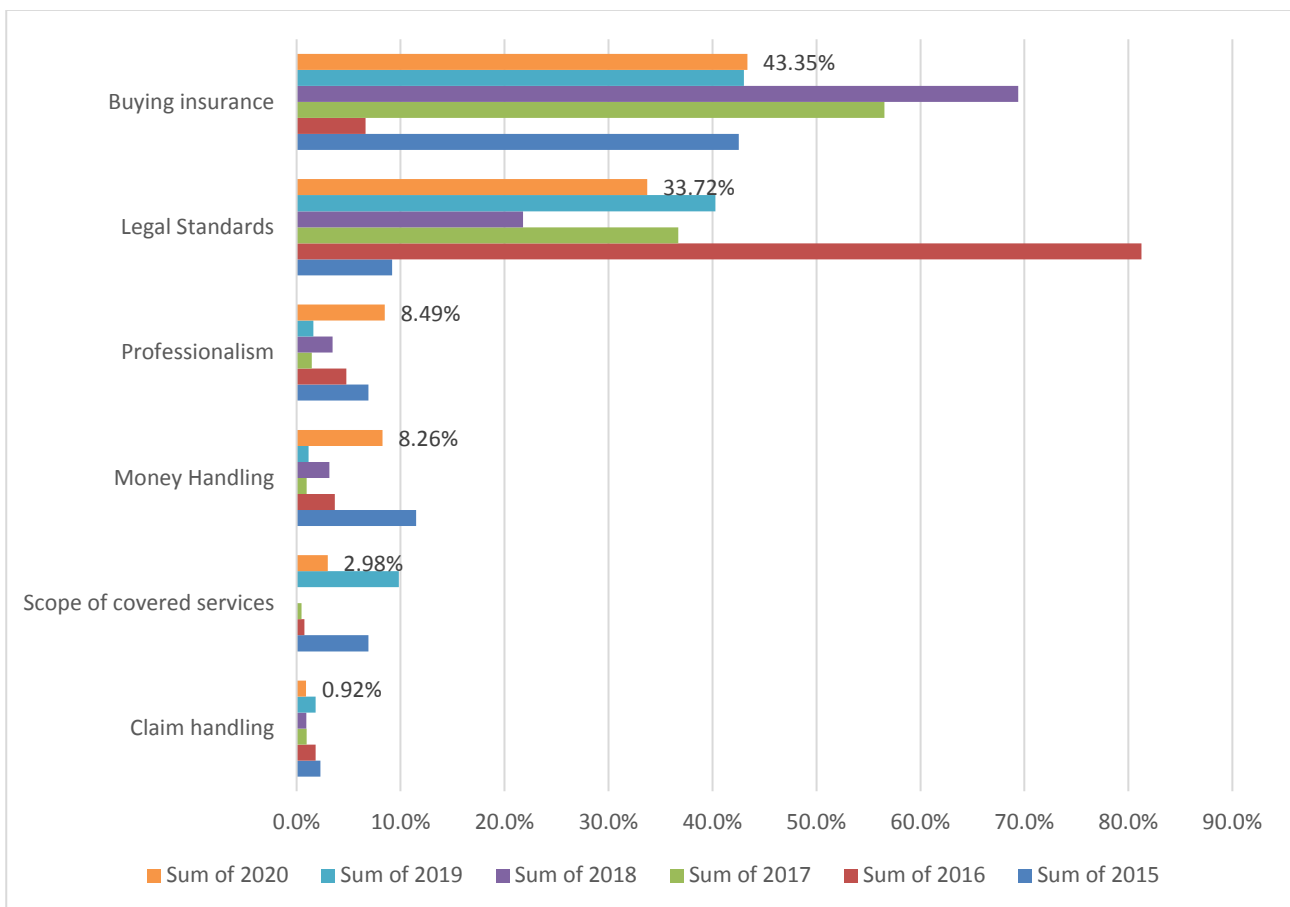


Data trend - Code subscribers in Category D

Table 9: Sector summary (Category D)

	2015	2016	2017	2018	2019	2020
Number of Code subscribers	35	28	39	32	25	32
Number of branches (including head office)	n/a	n/a	n/a	117	55	80
Total of self-reported Code breaches	87	249	177	375	376	436
Mean of self-reported Code breaches	1.9	8.6	5.9	11.7	15.0	14.1
% of Code subscribers self-reporting Code breaches	37%	57%	53%	50%	60%	71%
Total of self-reported IDR complaints	102	184	93	119	88	205
Mean of self-reported IDR complaints	3.2	6.6	3.1	3.7	3.5	6.6
% of Code subscribers self-reporting IDR complaints	80%	59%	63%	81%	64%	61.3%

Chart 7: Top six categories of Code breaches self-reported since 2015 in Category D

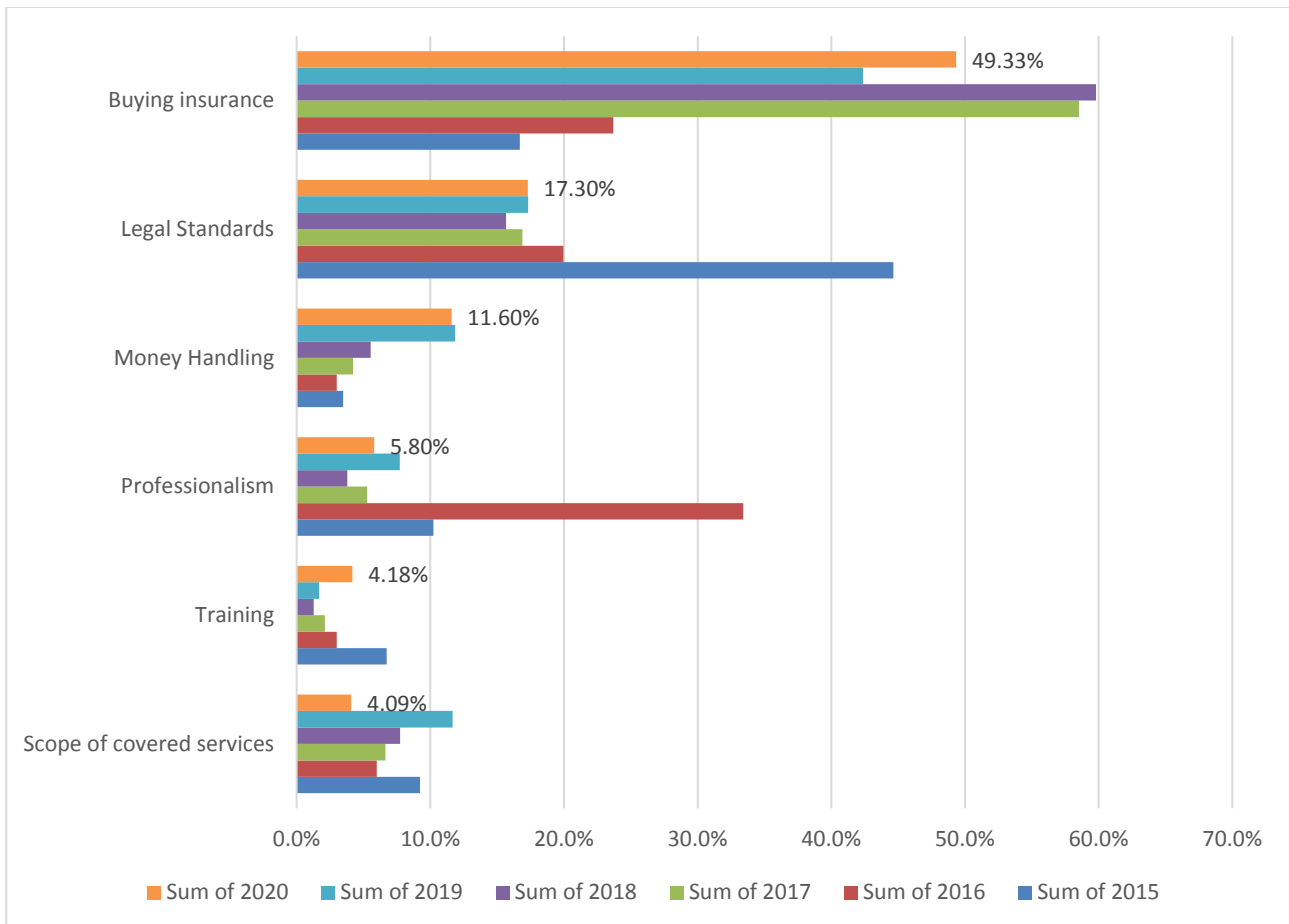


Data trend - Code subscribers in Category E

Table 10: Sector summary (Category E)

	2015	2016	2017	2018	2019	2020
Number of Code subscribers	249	216	194	183	177	332
Number of branches (including head office)	n/a	n/a	n/a	260	215	452
Total of self-reported Code breaches	629	510	704	677	549	1,052
Mean of self-reported Code breaches	2.3	2.3	3.5	3.7	3.1	3.2
% of Code subscribers self-reporting Code breaches	28%	33%	33%	35%	41%	34%
Total of self-reported IDR complaints	726	327	319	355	309	680
Mean of self-reported IDR complaints	2.2	1.5	1.6	1.9	1.7	2.1
% of Code subscribers self-reporting IDR complaints	39%	45%	44%	49%	47%	42.6%

Chart 8: Top six categories of Code breaches self-reported since 2015 in Category E



Appendix D: Self-reported Breach Data

Table 11: Number of Code subscribers (in % of total Code subscribers) self-reporting Code breaches since 2015

Number of self-reported Code breaches	2015	2016	2017	2018	2019	2020
Nil	68%	58%	59%	57%	49%	55.5%
1 to 10	26%	32%	31%	30%	35%	27.0%
11 to 20	4%	6%	4%	5%	7%	7.7%
21 to 50	2%	3%	4%	5%	7%	6.5%
51 to 100	0%	1%	1%	2%	1%	1.4%
Over 100	<1%	<1%	<1%	1%	1%	1.6%

Table 12: Number of self-reported Code breaches by size of Code subscriber in 2020

Number of self-reported Code breaches	Cat A	Cat B	Cat C	Cat D	Cat E	TOTAL ³⁶
Nil	3	6	5	9	215	238
1 to 10	5	4	14	13	80	116
11 to 20	3	3	6	1	20	33
21 to 50	6	3	4	6	9	28
51 to 100	0	0	4	1	1	6
Over 100	4	1	0	1	1	7

Table 13: Analysis of high volumes of self-reported Code breaches in 2020

Service Standard	Code subscribers who self-reported high number of breaches
Legal standards (St1)	<ul style="list-style-type: none"> 95 (22%) of total Code subscribers self-reported breaches of St1. More than half (59%) of Cat A and over half of Cat C (58%) subscribers self-reported breaches of St1. Two Cat A subscribers self-reported over half (55%) of breaches self-reported by that Category (99 and 41 breaches respectively). Two Cat D subscribers self-reported over three-quarter (77%) of breaches self-reported by that Category (83 and 30 breaches respectively). From the 95 Code subscribers self-reporting breaches of St1, two-thirds (58) self-reported no more than four breaches.
Conflict of interest (St2)	<ul style="list-style-type: none"> 5 (1%) of total Code subscribers self-reported breaches of St2. One Cat A subscriber self-reported six breaches of St2. The remaining subscribers self-reported one breach each of St2.
Who we act for (St3)	<ul style="list-style-type: none"> 5 (1%) of total Code subscribers self-reported breaches of St3. The five subscribers self-reporting one breach each of St3, included three Cat E, one Cat C and one Cat A subscriber.

³⁶ Some Code subscribers report as one entity and include all their Australian Financial Service Licences in one report.

Service Standard	Code subscribers who self-reported high number of breaches
Scope of covered services (St4)	<ul style="list-style-type: none"> • 43 (10%) of total Code subscribers self-reported breaches of St4. • Three Cat A and one Cat B subscriber each self-reported over 10 breaches each (e.g. 10, 12, 17 and 21 respectively).
Buying insurance (St5.1)	<ul style="list-style-type: none"> • 115 (27%) of total Code subscribers self-reported breaches of St5.1. • Over half of Code subscribers in each category self-reported breaches of St5.1 with the exception of Cat E where only 17% of subscribers self-reported breaches of St5.1. • One Cat A subscriber self-reported 162 breaches of St5.1 representing 33% of breaches of St5.1 of that category. • Two other subscribers of Cat A also represented high number of breaches of St5.1 (e.g. 93 and 77 respectively). • One Cat E subscriber self-reported 143 breaches of St5.1 representing 28% of breaches of St5.1 of that category.
Claims handling (St5.2)	<ul style="list-style-type: none"> • 29 (7%) of total Code subscribers self-reported breaches of St5.2. • One third (36%) of Cat A subscribers self-reporting breaches of St5.2, with one subscriber self-reporting 13 breaches (50% of breaches of St5.2 of that category).
Acting for insurer (St5.3)	<ul style="list-style-type: none"> • 7 (2%) of total Code subscribers self-reported breaches of St5.3. • One Cat C subscriber self-reported one third (21) of total breaches self-reported by all categories of St5.3.
Remuneration (St6)	<ul style="list-style-type: none"> • 25 (6%) of total Code subscribers self-reported breaches of St6. • One Cat C subscriber self-reported 10 breaches of St6. • Cat E is the category most represented, with 16 subscribers self-reporting breaches of St6.
Money handling (St7)	<ul style="list-style-type: none"> • 64 (15%) of total Code subscribers self-reported breaches of St7. • Two Cat A subscribers self-reporting one third (35%) of self-reported breaches by all Code subscriber of St7 (e.g. 58 and 72 respectively).
Training (St8)	<ul style="list-style-type: none"> • 29 (7%) of total Code subscribers self-reported breaches of St8. • About one quarter (5) of Cat A and one quarter (8) of Cat C subscribers self-reported breaches of St8. • Cat A and Cat E subscribers self-reported each about 50% of all breaches of St8 (e.g. 52 and 43 respectively). • Two Cat A subscribers had the highest number of self-reported breaches of St8 (e.g. 18 and 21 respectively).
Disasters (St9)	<ul style="list-style-type: none"> • None.
Dispute resolution (St10)	<ul style="list-style-type: none"> • 12 (3%) of total Code subscribers self-reported breaches of St10. • Cat E subscribers is the category most represented, with 7 subscribers self-reporting one breach each of St10. • One Cat A subscribers self-reported three breaches of St10.
Promotion of Code (St11)	<ul style="list-style-type: none"> • 4 (1%) of total Code subscribers self-reported breaches of St11. • Cat E subscribers is the category most represented, with two subscribers self-reporting five breaches each of St11.
Professionalism (St12)	<ul style="list-style-type: none"> • 33 (8%) of total Code subscribers self-reported breaches of St12. • Cat E subscribers is the category most represented in self-reporting breaches of St12. • One Cat A subscriber self-reported 23 breaches of St12 and one Cat D subscriber self-reported 28 breaches of St12, together nearly one third (29%) of all breaches self-reported of St12.

Table 14: Number of breach(es) by timeframe for immediate remedial action(s)

Row Labels	same day	48 hours	1 week	2 weeks	1 month	1 to 3 months	3 to 6 months	6 to 12 months	>1 year	other	Total
other	333	94	85	58	110	28	11	1	1	166	887
training	335	97	88	26	56	58	23	3	1	7	694
review of and changes to process	118	193	31	49	82	42	1	1	-	14	531
apology	325	40	38	16	12	4	-	4	-	5	444
undertaking	82	8	4	7	7	4	-	2	-	47	161
refund of premium	26	7	17	1	1	-	1	-	-	-	53
refund of fees/charges	16	4	12	2	1	-	1	1	-	-	37
ex-gratia payment	4	4	2	2	3	11	5	-	-	-	31
review and changes to terms and conditions	7	4	3	2	6	2	-	-	-	-	24
premium adjustment	5	1	-	1	1	1	-	2	-	1	12
Total	1,251	452	280	164	279	150	42	14	2	240	2,874

Table 15: Number of breach(es) by timeframe for long term remedial action(s)

Row Labels	within 1 month	1 to 3 months	3 to 6 months	6 to 12 months	other	Total
training	583	270	16	12	107	988
other	190	34	10	7	280	521
review of and changes to process	228	94	17	60	83	482
apology	66	4	1	-	8	79
undertaking	30	15	1	-	18	64
refund of fees/charges	2	2	21	-	1	26
refund of premium	6	-	-	-	-	6
premium adjustment	4	-	1	-	1	6
review and changes to terms and conditions	2	1	2	-	-	5
ex-gratia payment	-	1	-	-	1	2
Total	1,111	421	69	79	499	2,179

Appendix E: Root cause and impact of self-reported Code breaches in 2020

Table 16: Root causes of self-reported breaches by Code section in 2020

Note: numbers reflect incidents which in some cases would represent more than one breach. Not all Code subscribers provided conclusive information for each category.

<i>Code Standards (St)</i>	<i>Manual error</i>	<i>process and procedure not followed</i>	<i>other</i>	<i>incorrect process and procedure</i>	<i>system error/failure</i>	<i>staffing/resourcing issue</i>	<i>insufficient training</i>	<i>staff misconduct</i>	<i>mail house error</i>
St1 Legal standards	158	89	16	13	10	3	9	3	3
St2 Conflict of interest	7	1	1	-	-	-	-	-	-
St3 Who we act for	1	2	3	1	-	-	-	-	-
St4 Scope of covered services	42	28	8	6	8	-	1	-	-
St5 Buying insurance	325	143	213	28	23	20	9	16	1
St5 Claims handling	11	9	25	3	1	6	1	-	1
St5 Acting for insurer	1	1	1	-	2	-	1	-	-
St6 Remuneration	13	7	2	-	3	-	4	-	-
St7 Money handling	37	41	14	33	6	3	1	1	-
St8 Training	7	18	5	8	-	1	6	3	-
St9 Disasters	-	-	-	-	-	-	-	-	-
St10 Dispute resolution	1	5	4	-	2	1	-	-	-
St11 Promotion of Code	6	1	4	2	1	-	-	-	-
St12 Professionalism	41	29	4	8	-	3	4	7	-
Grand Total	650	374	300	102	56	37	36	30	5

Chart 9: Financial impact³⁷ to client(s) by root cause of self-reported breach(es)

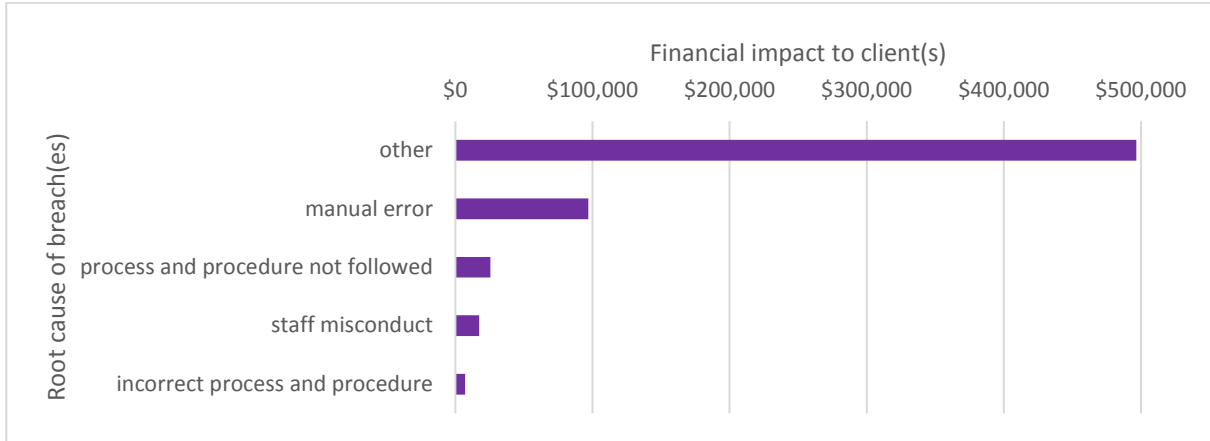


Chart 10: Number of client(s)³⁸ impacted by root cause of self-reported breach(es)

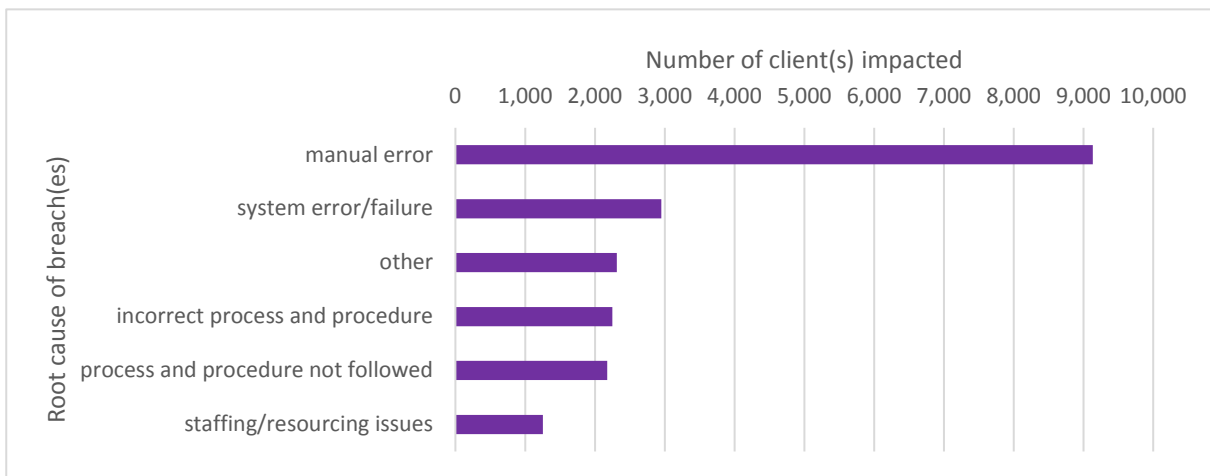
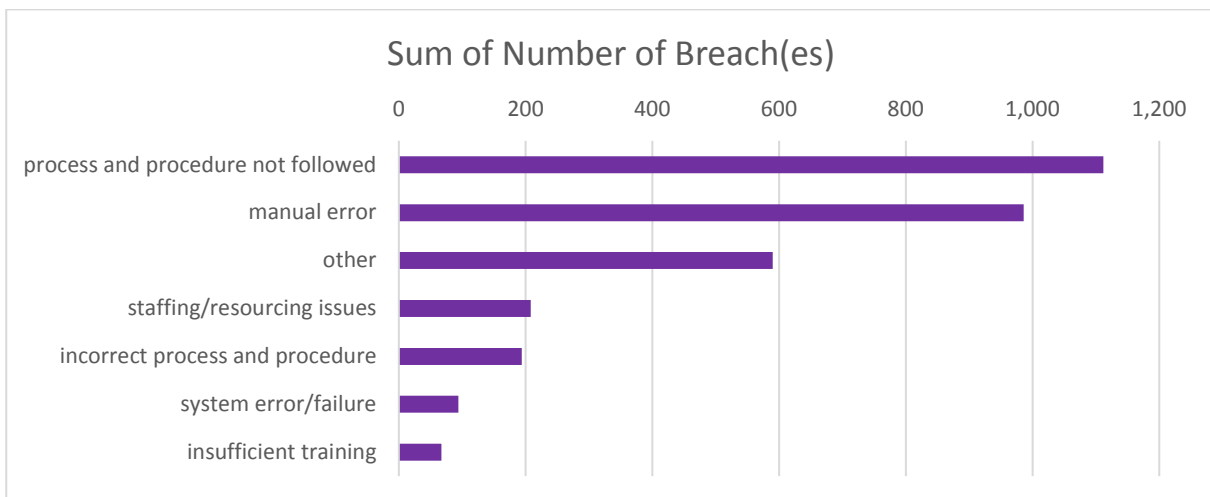


Chart 11: Number of self-reported breach(es)³⁹ by root cause



³⁷ Including root causes with over \$5,000 financial impact.

³⁸ Including root causes with over 1,000 clients impacted.

³⁹ Including root causes with over 50 self-reported breaches.

Table 17: Impact of self-reported breaches by Code section in 2020

Note: numbers are indicative, as not all Code subscribers provided conclusive information for each category.

	<i>Number of Client(s) impacted</i>	<i>Financial impact to client(s)</i>
St1 Legal standards	7,425	\$21,697
St2 Conflict of interest	8	\$0
St3 Who we act for	262	\$0
St4 Scope of covered services	301	\$5,693
St5 Buying insurance	3,095	\$294,618
St5 Claims handling	106	\$307,861
St5 Acting for insurer	28	\$0
St6 Remuneration	197	\$5,208
St7 Money handling	449	\$10,447
St8 Training	441	\$0
St9 Disasters	0	\$0
St10 Dispute resolution	7,006	\$0
St11 Promotion of Code	233	\$0
St12 Professionalism	1,189	\$6,067
Grand Total	20,740	\$651,592

Chart 12: Financial impact⁴⁰ to client(s) by Product/Service Types

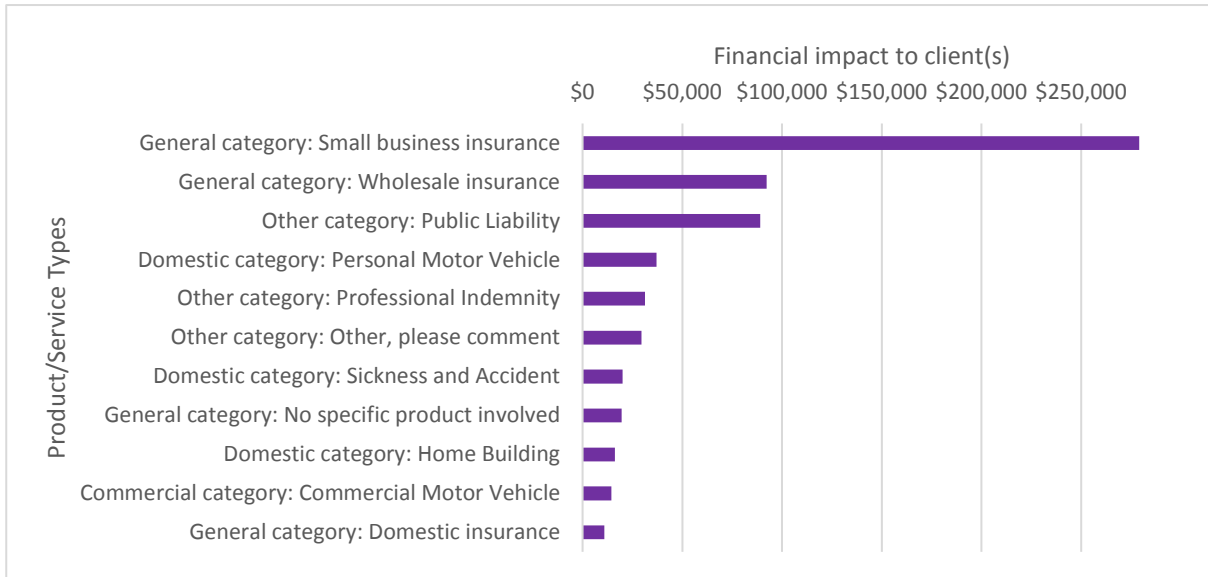


Chart 13: Number of client(s)⁴¹ impacted by Product/Service Types

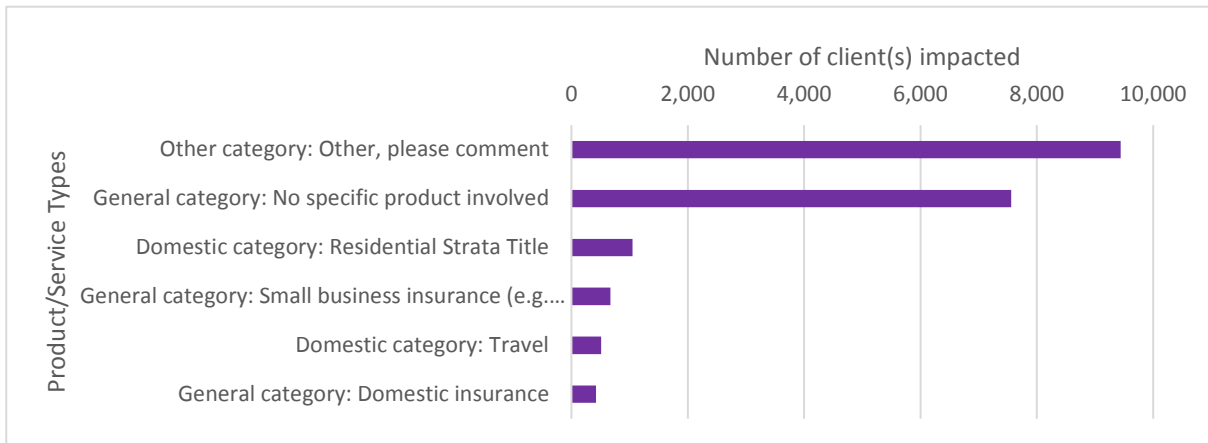
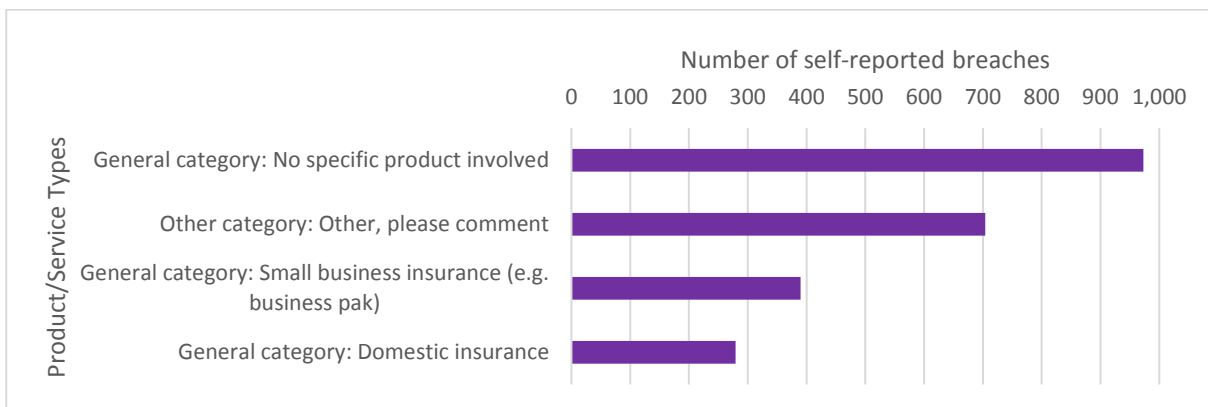


Chart 14: Number of self-reported breach(es)⁴² by Product/Service Type



⁴⁰ Including Product/Service Type with over \$20,000 financial impact.

⁴¹ Including Product/Service Type with over 1,000 clients impacted.

⁴² Including Product/Service Type with over 100 self-reported breaches.

Appendix F: Self-reported Complaints Data

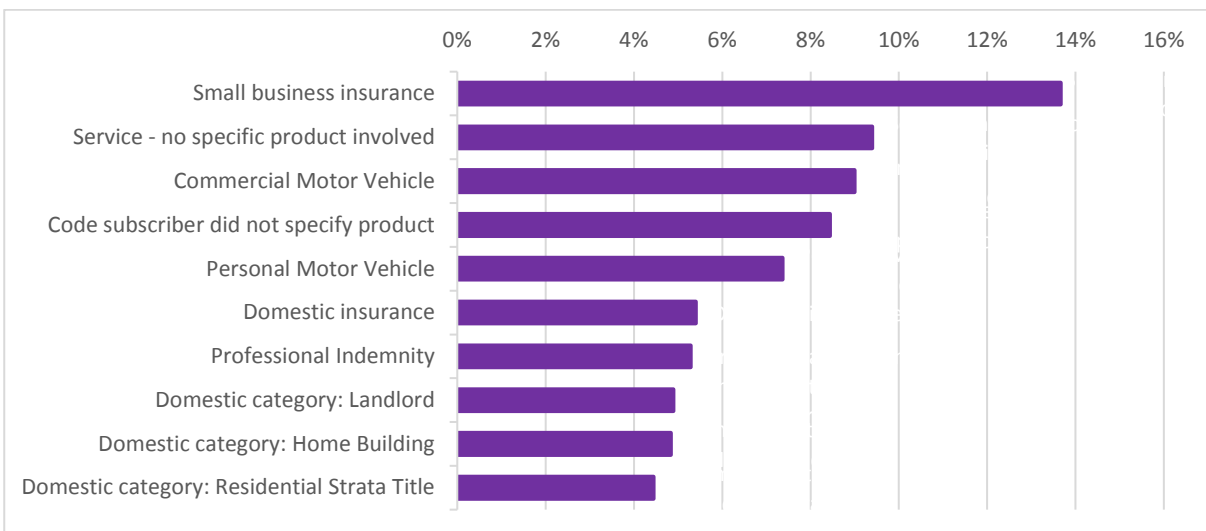
Table 18: Number of Code subscribers (in % of total Code subscribers) self-reporting complaints since 2015

Number of self-reported complaints	2015	2016	2017	2018	2019	2020
Nil	48%	46%	43%	39%	40%	48.0%
1 to 10	44%	46%	48%	51%	47%	42.4%
11 to 20	6%	6%	7%	7%	7%	5.1%
21 to 50	2%	1%	1%	2%	3%	3.2%
51 to 100	0%	<1%	1%	1%	1%	1.4%
Over 100	<1%	0%	0%	0%	<1%	0%

Table 19: Number of self-reported complaints by size of Code subscriber in 2020

Number of self-reported complaints	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Nil	1	2	3	12	190	208
1 to 10	10	11	23	14	126	184
11 to 20	3	3	3	3	10	22
21 to 50	4	1	4	1	4	14
51 to 100	4	0	0	1	1	6
Over 100	0	0	0	0	0	0

Chart 15: Top⁴³ product categories of total self-reported complaints in 2020



⁴³ Each reflecting over 4% of total self-reported complaints.

Chart 16: Top⁴⁴ issue categories of total self-reported complaints in 2020

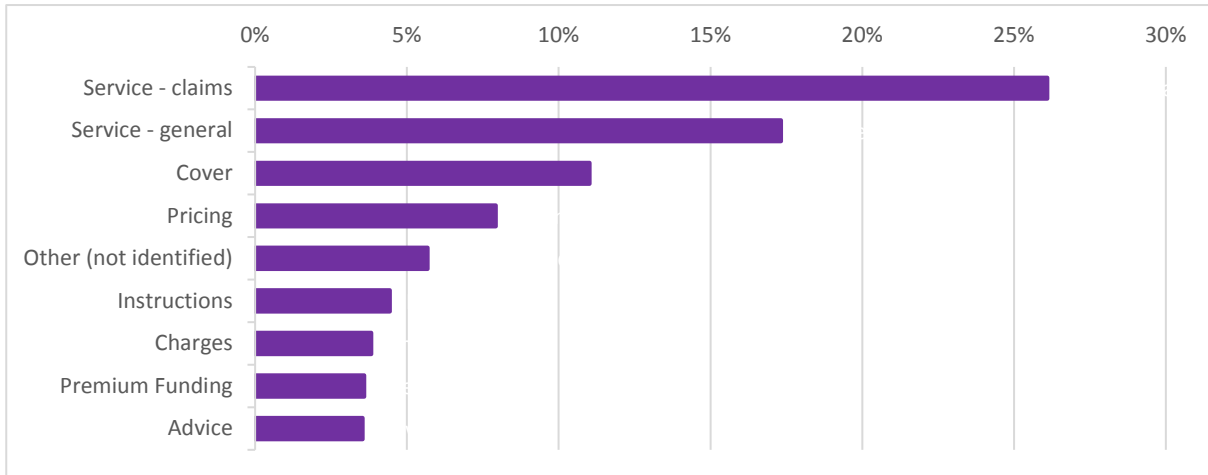


Chart 17: Top⁴⁵ outcome categories of total self-reported complaints in 2020

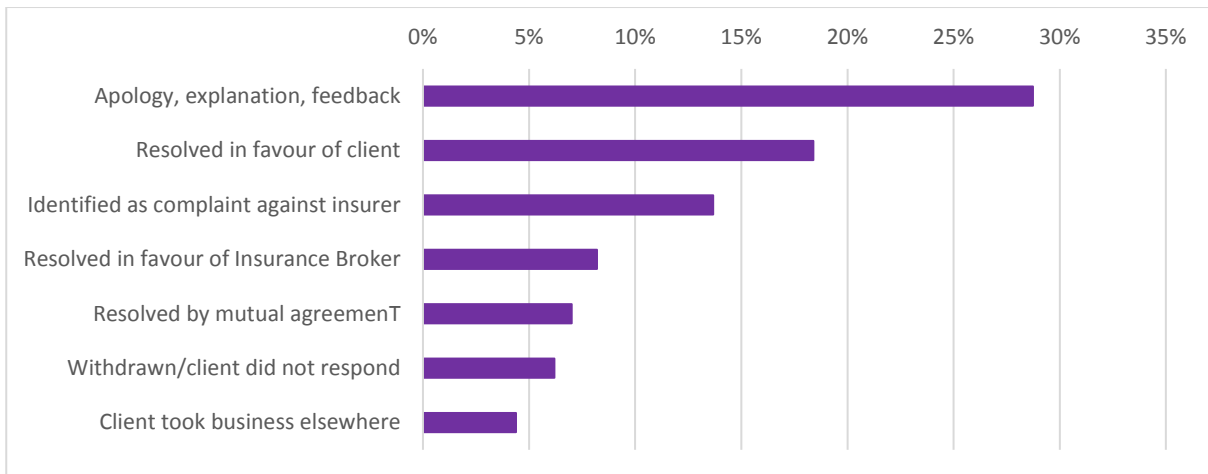
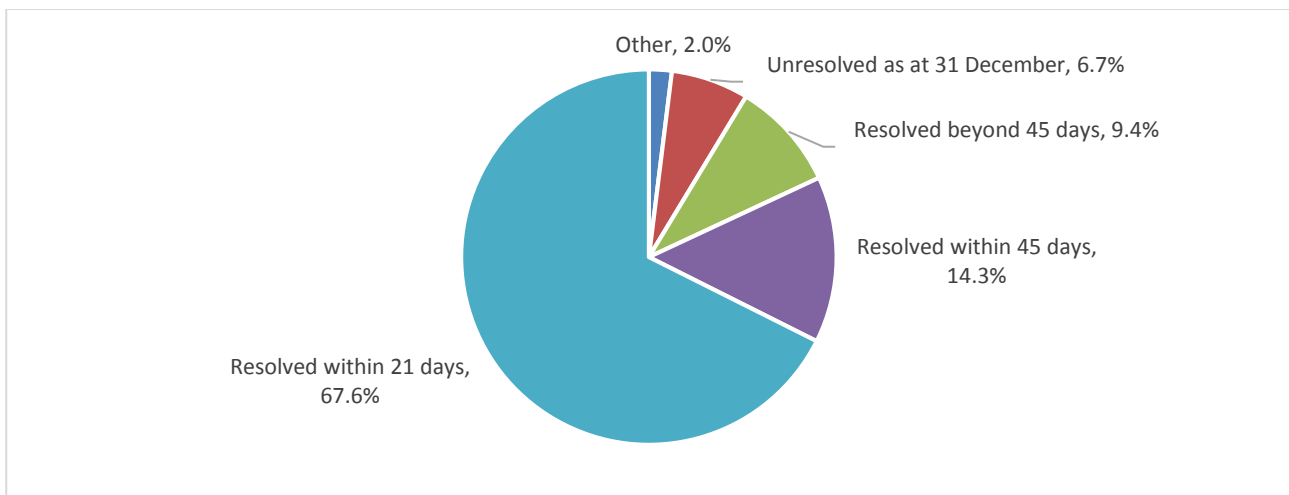


Chart 18: Resolution timeframe categories of self-reported complaints in 2020



⁴⁴ Each reflecting over 3% of total self-reported complaints.

⁴⁵ Each reflecting over 4% of total self-reported complaints.

Table 20: Analysis of high volumes of self-reported complaints in 2020

Complaints category	Details of high number of complaint categories
Product	
General category: Small business insurance (SB)	<ul style="list-style-type: none"> • 82 (19%) of total Code subscribers self-reported a total of 243 SB complaints. • About one in every seventh complaint (13.7%) involved SB. • About half of Cat A (59%), B (45%) and C (49%) subscribers self-reported SB complaints, and Cat D (19%) and Cat E (14%) subscribers to a lesser extent. • Cat E subscribers self-reported about half (103) of the total number of SB complaints and Cat A subscribers about one third (71).
Commercial category: Commercial Motor Vehicle (CMV)	<ul style="list-style-type: none"> • 44 (10%) of total Code subscribers self-reported a total of 160 CMV (9% of total) complaints. • About one third (36%) of Cat A subscribers self-reported Commercial CMV complaints. • Two individual Code subscribers self-reported the bulk of the CMV complaints (74): one Cat D subscriber self-reported one third (53) and once Cat C subscriber self-reported 13% (21) of the total CMV complaints.
Domestic category: Personal Motor Vehicle (PMV)	<ul style="list-style-type: none"> • 49 (11%) of total Code subscribers self-reported a total of 131 PMV (7.4% of total) complaints. • About one third (32%) of Cat A subscriber self-reported PMB complaints. • 27 Cat E subscribers self-reported nearly one third (56) of total PMV complaints, with one Cat E subscriber self-reported 11 PMV complaints.
General category: Domestic insurance	<ul style="list-style-type: none"> • 51 (12%) of total Code subscribers self-reported a total of 96 general domestic insurance (5.4% of total) complaints. • 8.3% of total complaints concerned this category. • Mainly Cat E subscribers (34) self-reported general domestic insurance complaints, representing over half (53) of total self-reported complaints.
Other category: Professional Indemnity (PI)	<ul style="list-style-type: none"> • 39 (9%) of total Code subscribers self-reported a total of 94 PI (5.3% of total) complaints. • Mainly Cat A subscribers (10) self-reported PI complaints representing about half (42) of total self-reported complaints, including one Cat A subscribers self-reporting 18 PI complaints.
Issue	
Service – claims	<ul style="list-style-type: none"> • 120 (28%) of total Code subscribers self-reported a total of 464 claims service complaints, about one quarter (26.1%) of total complaints. • Over three quarters of Cat A (82%) and Cat C (76%) subscribers self-reported claims service complaints, but only 18% of Cat E subscribers self-reported claims service complaints. • Nearly one third of total complaints (150) were self-reported by Cat A subscribers.
Service – general	<ul style="list-style-type: none"> • 91 (21%) of total Code subscribers self-reported a total of 308 general service (17.3% of total) complaints. • More than half of Cat A (68%), Cat B (53%) and Cat C (48%) self-reported general service complaints. In comparison 16% of Cat E subscribers self-reported general service complaints.

Complaints category	Details of high number of complaint categories
	<ul style="list-style-type: none"> • Cat A (103) and Cat E (102) subscribers self-reported each on third of total general service complaints.
Cover	<ul style="list-style-type: none"> • 73 (17%) of total Code subscribers self-reported a total of 196 cover (11% of total) complaints. • Most Code subscribers self-reported no more than once complaint regarding a cover issue. • One Cat D subscriber self-reported 18 complaints regarding cover issues.
Pricing	<ul style="list-style-type: none"> • 44 (10%) of total Code subscribers self-reported a total of 141 pricing (7.9% of total) complaints. • Most pricing complaints were self-reported by Cat E subscribers, with one Cat E subscriber self-reporting 34 issues.
Outcome	
Apology, explanation and/or acknowledgment of feedback	<ul style="list-style-type: none"> • 115 (27%) of total Code subscribers self-reported a total of 511 complaints resolved by apology, about one quarter (28.7% of total) complaints. • Over half (244) of complaints resolved by apology were self-reported by Cat E subscribers. • Once Cat A and three Cat E subscribers self-reported that over 20 complaints were resolved by apology.
Resolved in favour of the client	<ul style="list-style-type: none"> • 75 (18%) of total Code subscribers self-reported a total of 327 complaints resolved in favour of the client, about one in every fifth (18.1% of total) complaints. • 15% of Code subscribers reported this outcome via IDR, 3% reported outcome via EDR. • One Cat E subscriber (61) and one Cat A subscriber (32) self-reported a high number of complaints resolved in favour of the client.
Identified as complaint against insurer	<ul style="list-style-type: none"> • 74 (17%) of total Code subscribers self-reported a total of 243 complaints identified as a complaint against an insurer (13.7% of total complaints). • Most of the complaints identified as a complaint against an insurer were self-reported by Cat E subscribers, including one Cat E subscribers self-reporting 15 complaints in this category.
Resolved in favour of Insurance Broker	<ul style="list-style-type: none"> • 52 (12%) of total Code subscribers self-reported a total of 146 (8.2% of total) complaints resolved in favour of the insurance broker. • 7% of Code subscribers reported this outcome via IDR, 5% reported outcome via EDR.
Resolved by mutual agreement	<ul style="list-style-type: none"> • 53 (12%) of total Code subscribers self-reported a total of 125 (7% of total) complaints resolved by mutual agreement. • 10% of Code subscribers reported this outcome via IDR, 2% reported outcome via EDR.
Withdrawn/ client did not respond	<ul style="list-style-type: none"> • 52 (12%) of total Code subscribers self-reported a total of 110 (6.2% of total) complaints as withdrawn and/or where the client did not respond to any further attempts to resolve the matter. • Most complaints in this category were self-reported by Cat A subscribers.

Complaints category	Details of high number of complaint categories
Timeframe	
Resolved within 21 days	<ul style="list-style-type: none"> • 186 (44%) of total Code subscribers self-reported a total of 1,202 (67.6% of total) complaints as resolved within 21 days. • One Cat E subscriber self-reported the highest number of complaints (66) as resolved within 21 days.
Resolved within 45 days	<ul style="list-style-type: none"> • 74 (17%) of total Code subscribers self-reported a total of 255 (14.3% of total) complaints resolved within 45 days. • Mainly Cat A subscribers self-reported a high number of complaints resolved within 45 days.
Resolved beyond 45 days	<ul style="list-style-type: none"> • 64 (15%) of total Code subscribers self-reported a total of 167 (9.4% of total) complaints resolved beyond 45 days. • Mainly Cat A subscribers self-reported a high number of complaints resolved beyond 45 days. • Main reasons for the delay were noted as the complexity of the matter, the client not providing sufficient information in time and the matter being referred to AFCA.

Appendix G: Compliance monitoring activities in 2020

Table 21: Compliance monitoring activities undertaken by Code subscribers

Note: figures represent percentage of Code subscribers in that category who stated that they undertook a compliance monitoring activity in that particular area in 2020.

Code monitoring activity	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Code information available on your website and branches	86%	65%	73%	69%	49%	55%
Information on your internal dispute resolution (IDR) process on your website	86%	65%	76%	69%	46%	53%
Information on your external dispute resolution (EDR) process on your website	86%	65%	73%	59%	47%	53%
Checklist outlining IDR timeframes	73%	59%	58%	50%	36%	41%
Managing conflict of interest	91%	65%	76%	75%	55%	60%
Transparent disclosure of third-party providers to client(s)	41%	47%	52%	50%	38%	40%
Transparent disclosure of fees and commissions to client(s)	77%	59%	70%	59%	55%	58%
Implementation of remuneration arrangements	41%	47%	30%	25%	24%	26%
Review of % of financial results attributing to incentives to ensure that financial results are not the sole driver of reward outcomes	32%	41%	36%	34%	27%	29%
Training of staff	91%	94%	91%	91%	85%	87%
Training of authorised representatives	91%	71%	64%	44%	37%	44%
Training of third-party providers (e.g. claims recovery services, debt collectors, lawyers, valuers, claims preparation companies and other professionals)	23%	6%	9%	16%	10%	11%
Privacy obligations	86%	65%	61%	66%	53%	57%
Sale of add-on general insurance products	36%	35%	9%	13%	15%	16%
Renewal procedures	73%	71%	67%	78%	70%	70%
Dealing with clients in financial difficulty	64%	65%	61%	69%	59%	60%
Identifying and assisting clients affected by family violence	36%	47%	36%	47%	23%	28%
Identifying and assisting clients affected by elder abuse	23%	29%	21%	38%	17%	20%
Other	9%	6%	6%	6%	5%	6%

Note:

Code subscribers reported the following compliance monitoring activities under the category 'other':

- Enhanced liability assessments tracked on motor business to ensure clients receive entitlements to hire cars.
- Restructure following sale of part of broking portfolio.
- Active compliance management and review of the Breach and Complaints Register with board oversight and engagement with executive management.
- Open communication channels to report on non-compliance.
- Ongoing activities to encourage strong compliance culture through staff engagement initiatives, team sessions and compliance presence in meetings/discussions.
- Internal audits to ensure processes, procedures and behaviours adhere to the Code and legislative requirements.
- Implemented new Complaints Management Policy and Procedure to comply with Code and AFCA procedures.
- Review of assistance provided in extending premium funding instalments.
- Internal review and audit of client files.
- Development of Policy and Procedure for management of complaints in line with new APRA and Code guidelines.
- Created position of a full-time role as Compliance Officer.