

# **Compliance with section 6.3 of the Life Insurance Code of Practice**

**Report on an own motion inquiry into Life  
subscribers' compliance with section 6.3 of the  
Life Insurance Code of Practice**

**January 2022**

# Contents

<b>Overview Summary</b>	<b>3</b>
Purpose	3
Background	3
Section 6.3 requirements and importance for customers	4
Summary of key findings	5
Conclusions	6
Summary of Recommendations	7
<b>Section 6.3 of the Code</b>	<b>8</b>
Elements of section 6.3	8
Scope of section 6.3	8
<b>Data collection</b>	<b>8</b>
<b>Findings</b>	<b>9</b>
Size of the market (Question 1 & 2)	9
On-sale products	9
Off-sale products	10
Number of customers covered by on-sale and off-sale products	11
Type of processes used (Question 3 & 4)	11
Processes used in relation to the Timeframe element	12
Processes used in relation to the Information element	13
Compliance framework (Question 5)	14
Breach data (Question 6)	15
Number of breaches	15
Number of customers impacted	16
Breaches in relation to on-sale vs off-sale products	17
Breaches in relation to automated vs manual processes	17
Breaches in relation to the Timeframe element and Information element	17
Significant vs not significant breaches	18
Reasons for the breaches	19
Communication method (Question 7)	20
<b>Observations and recommendations</b>	<b>21</b>
Importance of the off-sale market	21
Implementation of automated processes and monitoring and review of systems and processes	22
Issuing of annual notices	23
Reporting of significant breaches of section 6.3	23
<b>Conclusion</b>	<b>25</b>
<b>Annexure</b>	<b>26</b>
What is an OMI?	26

# Overview Summary

## Purpose

The purpose of this report is to outline the findings of an Own Motion Inquiry (OMI) conducted by the Life Code Compliance Committee (the Committee) to assess subscribers' compliance with section 6.3 of the Life Insurance Code of Practice (the Code).

The findings and recommendations in this report are based on:

- analysis of data provided by 18<sup>1</sup> subscribers in responses to a questionnaire developed by the Committee regarding products, systems and processes, practices and breaches relating to section 6.3 of the Code, covering the period 1 January 2019 to 31 December 2020;
- analysis of data collected from subscribers on compliance with provisions of the Code through the Committee's annual data collection processes; and
- lessons learned from the Committee's investigations of alleged breaches of section 6.3.



**6 significant breaches of section 6.3 received by the Committee since March 2021**

## Background

The Committee initiated the OMI having identified that compliance with the obligation to provide customers with a compliant annual notice has been a consistent issue for subscribers since the commencement of the Code in 2017. The Committee had been notified of 21 significant breaches of section 6.3 between July 2017 and December 2020 and was concerned about the impact of non-compliance with section 6.3 on customers. The Committee was also concerned about possible under reporting of significant breaches of section 6.3 of the Code.

<sup>1</sup> While the Committee requested data from 19 subscribers, 1 subscriber only issued Group policies. As Group policies are not covered by the obligations in section 6.3 of the Code, the subscriber was not able to provide the Committee with any relevant data.

## Section 6.3 requirements and importance for customers

Section 6.3 relates to subscribers' obligation to provide customers<sup>2</sup> with an annual notice in writing each year prior to the anniversary of the life insurance policy. This is referred to in this report as the **Timeframe element** of section 6.3.

Section 6.3 also requires subscribers to include important information about the customer's policy to the customer in the annual notice. This is referred to in this report as the **Information element** of section 6.3 in this report. The Information element of section 6.3 requires subscribers to include the following information in their annual notices to customers:

- the types of cover that the customer has;
- how much the customer is insured for;
- an explanation for any increase in premiums;
- information about the risks of cancelling and replacing a policy;
- how to contact the subscriber to discuss options if the customer wants to change the terms of the policy or is having difficulty meeting their payments; and
- what to do in the event of a claim.

Providing this information serves to remind customers of their cover and prompt them to consider if their cover is appropriate for their current circumstances. The annual notice is often the only readily available source of information for customers regarding their life insurance policies and provides much needed clarity to customers on the specifics and cost of their cover. Failure to issue the annual notice on time or failure to include all relevant information in annual notices can adversely impact customers.

For example, if customers do not get the notice before the renewal date and they have not set up a direct debit or a direct debit is incorrect or has changed, their policy might inadvertently lapse. If customers cannot afford the premium, and they don't receive the annual notice on time and with the required information, they miss receiving the prompt of contacting the insurer to discuss or consider whether the policy is still suitable. If all required information is not included in the annual notice, customers cannot assess if their policy is appropriate or affordable for their circumstances.

“ Failure to issue the annual notice on time or failure to include all relevant information in annual notices can adversely impact customers.

<sup>2</sup> As part of its data collection, the Committee has defined a 'customer' to be the life insured or policy owner who is entitled to receive the annual notice on the policy. A person with multiple policies will be counted as multiple customers.

**Summary of key findings** As at 31 December 2020, responses of 18 subscribers to the LCCC's OMI questionnaire on section 6.3 processes, practice and compliance identified that:

**7.8m** ANNUAL NOTICES WERE ISSUED BY SUBSCRIBERS BETWEEN 1 JANUARY 2019 AND 31 DECEMBER 2020

**60%** OF ANNUAL NOTICES WERE DELIVERED VIA POST AND 40% VIA EMAIL

**18** subscribers reported a total of:

**106** ON-SALE PRODUCTS **and** **1,336** OFF-SALE PRODUCTS

Most subscribers used automated processes to generate annual notices that are compliant with both the Timeframe and Information elements of section 6.3 of the Code.



> Timeframe element

**103** 97% ON-SALE PRODUCTS

**1,295** 97% OFF-SALE PRODUCTS



> Information element

**76** 72% ON-SALE PRODUCTS

**898** 67% OFF-SALE PRODUCTS

Customers covered

**1.8m**

ON-SALE PRODUCTS

**2.5m**

OFF-SALE PRODUCTS

**76** breaches of section 6.3 of the Code recorded by subscribers between 1 January 2019 and 31 December 2020

IMPACTING ALMOST 

**200,000** customers

**29 of the 76 breaches were significant breaches<sup>3</sup>.** The 29 significant breaches impacted almost 180,000 customers, or more than 90% of all customers affected by the reported 76 breaches. 28 of the 29 significant breaches related to automated processes.

**65 (86%) of the 76 breaches related to automated processes** and 11 (14%) of the 76 breaches related to manual processes.

**35 (46%) breaches related to the Timeframe element,** 31 (41%) breaches related to the Information element and 10 (13%) breaches involved both elements.

**System issues accounted for 42 (55%) breaches,** human error accounted for 18 (24%) breaches, and compliance processes accounted for 16 (21%) breaches.

**Some subscribers did not identify** and report some significant breaches of section 6.3 prior to the section 6.3 OMI inquiry, suggesting that some subscribers may not have robust processes and procedures in place for monitoring and identifying breaches of section 6.3 of the Code.

<sup>3</sup> The Committee notes that 29 breaches of section 6.3 reported to the Committee as part of its data collection for the section 6.3 OMI have been deemed to be significant by subscribers. However, a number of these significant breaches have yet to be reported to the Committee as a significant breach of the Code. The Committee notes that section 13.4 of the Code requires subscribers to self-report a significant breach of the Code within 10 business days of identifying the significant breach. The Committee expects subscribers to have robust processes in place to identify and report any instances where a significant breach has occurred.

## Conclusions

The Committee appreciates and thanks subscribers for taking the time and effort to provide data and information about their systems, processes and practices regarding compliance with section 6.3 of the Code. The level of cooperation of subscribers and information they provided confirms that most subscribers are taking seriously their Code obligations and have put in place systems, processes and practices to ensure compliance with section 6.3.

Noting that most customers covered by life insurance products that are subject to section 6.3 requirements were not impacted by breaches of section 6.3 of the Code, the Committee was nonetheless concerned that 198,000 customers were impacted by 76 breaches of the Code, including 29 significant breaches. While this number and percentage of customers may be small in comparison with the overall number of customers with policies covered by subscribers' section 6.3 obligations, the Committee is concerned that each breach can have a significant impact on individual customers.

A breach of the Timeframe or Information element of section 6.3 can impact affected customers' financial circumstances and their capacity to assess the affordability and suitability of their policies and take appropriate action as necessary. The impact of a breach of the Timeline or Information elements of section 6.3 can be particularly detrimental for customers whose policies are no longer appropriate to their circumstances or who are experiencing difficulty in

meeting payments. These are the people the Code is designed to protect, and the industry needs to take seriously its obligations to these customers. Subscribers need to ensure that their processes and practices reflect, as a minimum, the safeguards and protections prescribed in section 6.3 of the Code.

The information provided to the Committee identified that most breaches related to systems issues, human error and failures in subscribers' management of their section 6.3 processes. The Committee notes that any process is only as good as its weakest link, and subscribers need to regularly test and assess their systems and processes to ensure they are current and sufficiently robust, reliable and effective to enable compliance with the obligations in the Code. Subscribers also need to provide ongoing training for staff in Code requirements and practices to ensure compliance with subscribers' obligations under the Code.

In the interests of supporting and assisting subscribers in meeting their obligations under the Code and in encouraging continuous improvement of processes and practice, this report of the OMI of section 6.3 has identified areas for improvement to mitigate the risk of subscriber non-compliance in relation to both the Timeframe and Information elements of section 6.3, and the resulting adverse impact on customers.

## Summary of Recommendations

The Committee is making a number of observations and recommendations to support subscribers in ensuring compliance with section 6.3 of the Code and implementing continuous improvement of their systems, processes and practices. The observations and recommendations focus on:

- Robustness of processes in relation to off-sale products
- Implementation of automated processes and monitoring and review of systems and processes
- Strengthened safeguards in relation to issuing of annual notices
- Reporting of significant breaches

### RECOMMENDATION 1

The Committee **recommends** that subscribers review their processes for managing compliance with section 6.3 in relation to all off-sale products as well as on-sale products to ensure they remain current, accurate, robust and effective in meeting subscribers' obligations to meet both the Timeframe and Information elements of section 6.3 of the Code and to enable early detection of breaches to minimise the impact on affected customers.

### RECOMMENDATION 2

The Committee **recommends** that subscribers consider adopting automated processes or enhanced controls over manual processes for all on-sale and off-sale products to enable compliance with section 6.3 of the Code, in relation to both the Timeframe and the Information elements.

### RECOMMENDATION 3

The Committee **recommends** that subscribers' planning and implementation of system changes and upgrades and related change management processes encompass checks, tests and assurances that the automated generation and issuing of annual notices complies with the Timeframe and Information elements of section 6.3 of the Code for all products.

### RECOMMENDATION 4

The Committee **recommends** that subscribers not only monitor automated systems and processes used to ensure compliance with section 6.3 but also review the content of templates and communications used in relation to issuing annual notices to customers, to ensure all the information required under section 6.3 is accurately provided to customers.

### RECOMMENDATION 5

The Committee **recommends** that, irrespective of whether subscribers issue annual notices by post or digitally, they should have processes in place to maintain the currency and accuracy of all customers' postal and digital addresses, to ensure that annual notices are issued to customers in accordance with the Timeline and Information requirements of section 6.3 and to minimise the risk of inadvertent disclosure of personal information to third parties.

### RECOMMENDATION 6

The Committee **recommends** that all subscribers ensure they have robust and effective processes to monitor compliance with section 6.3 of the Code, identify breaches and report significant breaches to the Committee where appropriate and take immediate action to notify affected customers and rectify identified breaches as quickly as possible.

# Section 6.3 of the Code

## Elements of section 6.3

Section 6.3 sets out 2 separate elements for Code subscribers:

- **Timeframe element:** Subscribers are required to provide the customer with an annual notice in writing each year prior to the anniversary of the customer's life insurance policy.
- **Information element:** Subscribers are required to ensure that the annual notice includes:
  - a. the types and amount of cover;
  - b. an explanation for any increase in premiums;
  - c. information about the risks of cancelling and replacing an existing policy;
  - d. information about how to contact the subscriber to discuss options if the customer wants to change the terms of the policy or is having difficulty making payments; and
  - e. what to do in the event of a claim.

## Scope of section 6.3

Section 6.3 applies to all products (both on-sale and off-sale) that are currently active and have policies that are currently in force, other than Consumer Credit Insurance (CCI) products or products sold through the Group distribution channel.

## Data collection

The Committee collected data from 18 subscribers in relation to:

- All active products with policies in force as at 31 December 2020
- The types of processes that subscribers had in place to ensure compliance with both the Timeframe and Information elements in section 6.3 of the Code
- Breaches of section 6.3 of the Code during the period 1 January 2019 to 31 December 2020.

A customer is defined as the person eligible to receive the annual notice for a policy and is usually the policy owner. As such, an individual with multiple policies will be counted as multiple customers.

Industry data was collected via a 7-part questionnaire. The 7 questions addressed:

1. The size of the market for on-sale products.
2. The size of the market for off-sale products.
3. The types of processes used for the Timeframe element of section 6.3.
4. The types of processes used for the Information element of section 6.3.
5. Framework to enable ongoing compliance with section 6.3 of the Code.
6. Breach data relating to section 6.3 of the Code.
7. The method of communicating the annual notice to customers.



# Findings

## Size of the market (Question 1 & 2)

Subscribers were asked to provide information about the number of on-sale and off-sale products they offered as at 31 December 2020, as well as the number of customers who held these products.

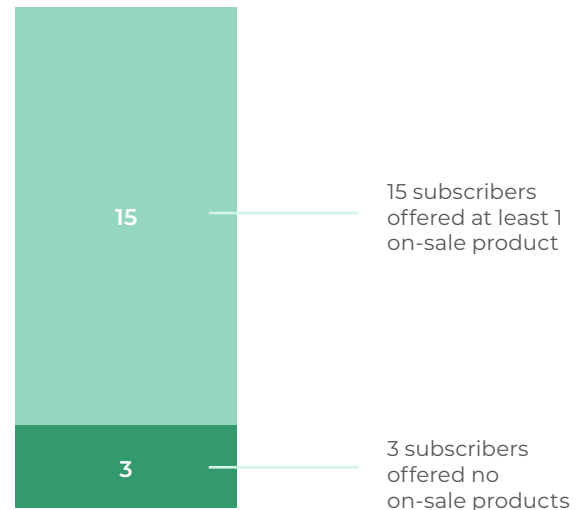


### ON-SALE PRODUCTS

18 subscribers reported a total of 106 on-sale products as at 31 December 2020.

- 15 subscribers offered at least 1 on-sale product.
- 3 subscribers offered no on-sale products for purchase due to product consolidation post mergers with other life insurers.

Subscribers have conducted significant consolidation of their on-sale books, with only 5 subscribers offering more than 10 on-sale products, and the highest number of on-sale products from a single subscriber amounting to 18 products.



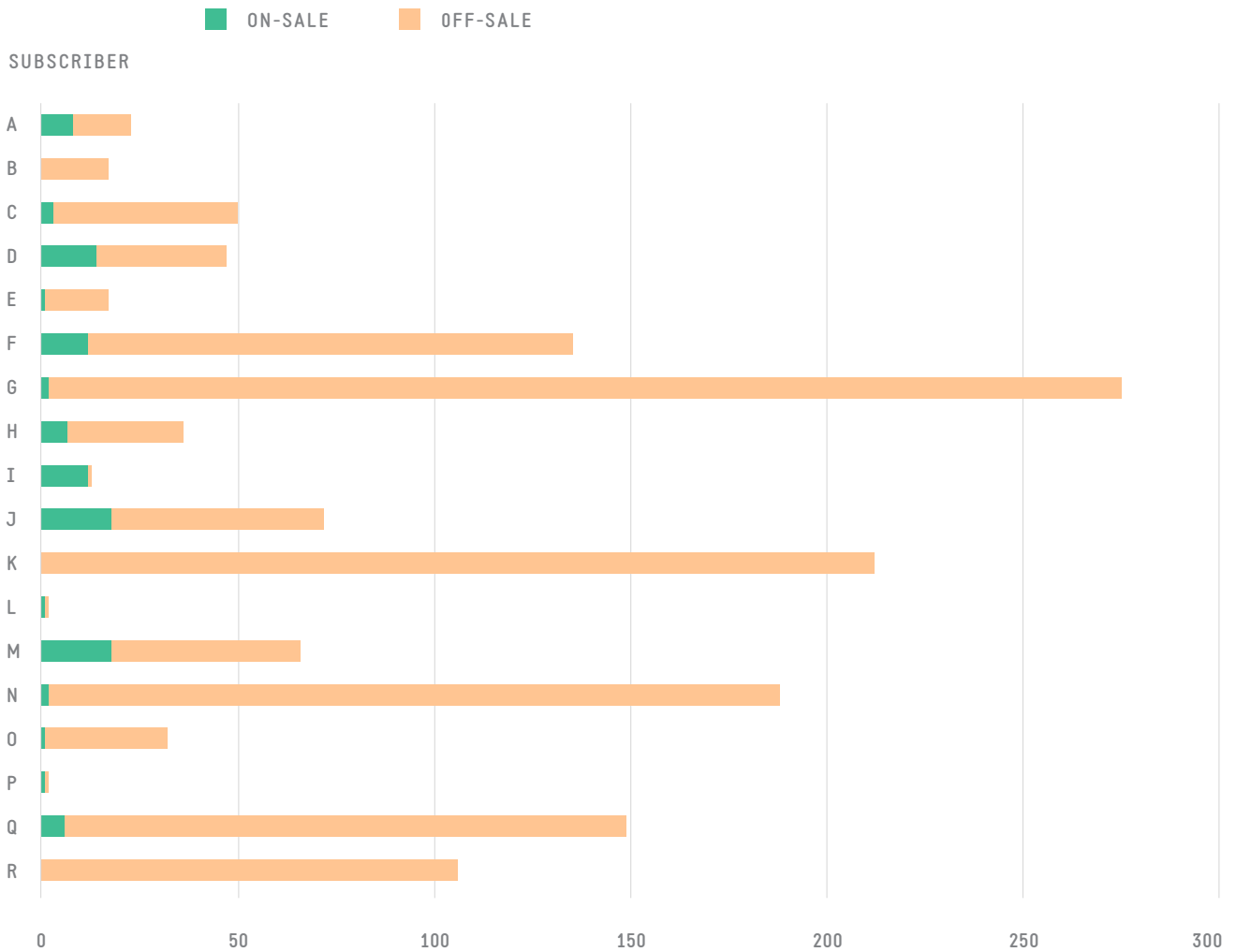
“ Subscribers were asked to provide information about the number of on-sale and off-sale products they offered as at 31 December 2020, as well as the number of customers who held these products.

## OFF-SALE PRODUCTS

In contrast, the 18 subscribers reported a total of 1,336 off-sale products as at 31 December 2020, with 6 subscribers having books of more than 100 off-sale products each. The highest number of off-sale products from a single subscriber was 273 (Figure 1).

FIGURE 1.

Number of on-sale and off-sale products as at 31 December 2020

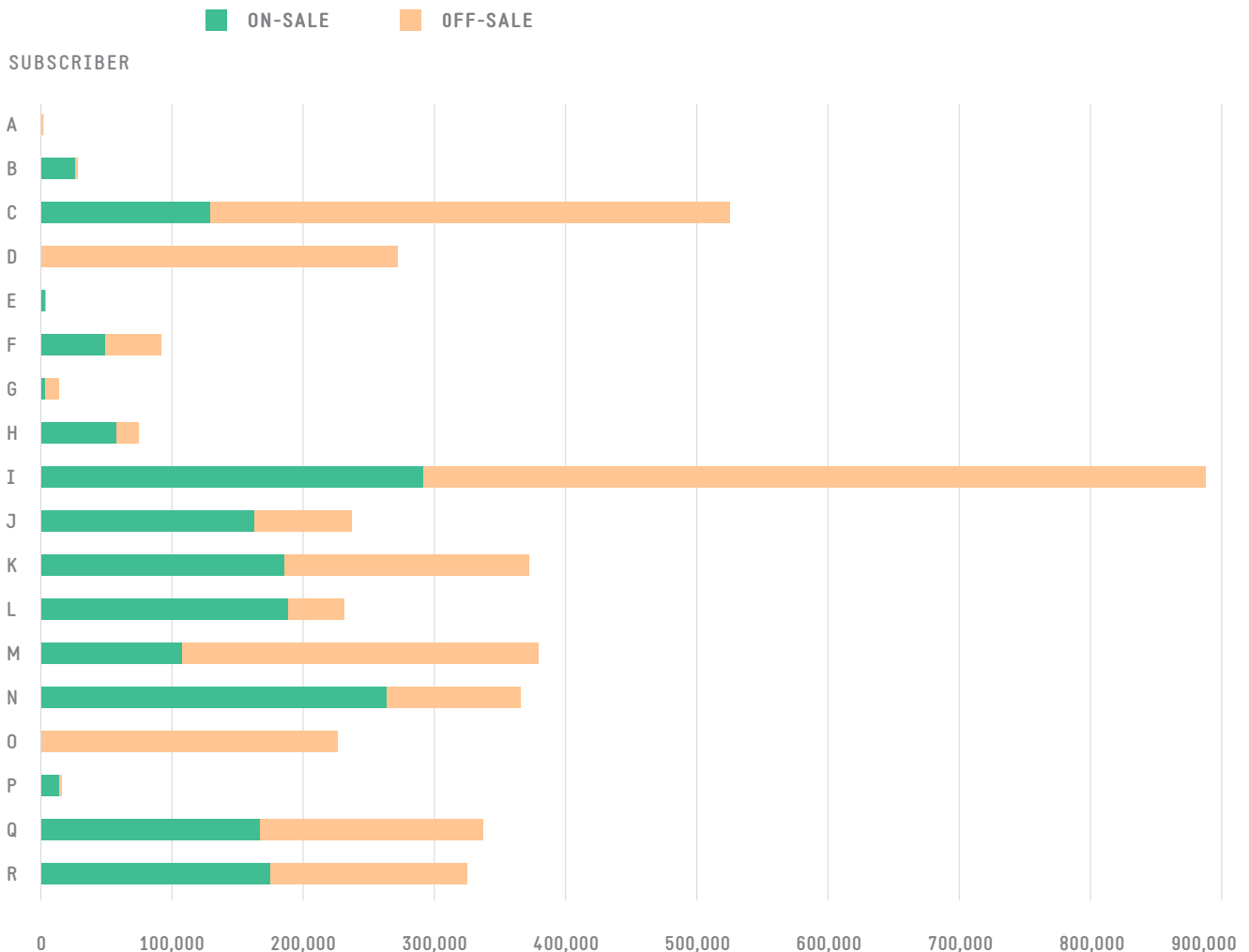


## NUMBER OF CUSTOMERS COVERED BY ON-SALE AND OFF-SALE PRODUCTS

In relation to the number of customers covered by the products, the 106 on-sale products covered 1.8m customers, while the 1,336 off-sale products covered 2.5m customers (Figure 2).

FIGURE 2.

### Number of customers as at 31 December 2020



## Type of processes used (Question 3 & 4)

Subscribers were asked to report on the types of processes used in relation to both the Timeframe element and the Information element of section 6.3, and to classify whether a process was automated or manual. An automated process is defined as a process or procedure that is performed without substantial human intervention, such as a system which automatically

notifies the user that an annual notice letter for a customer is due in addition to generating and populating the letter.

In contrast, a manual process is a process or procedure that requires substantial human intervention to function, such as a process where human intervention is required to notify the user and generate the letter.



**97%**

**of on-sale products used an automated process for the Timeframe element of section 6.3**

### PROCESSES USED IN RELATION TO THE TIMEFRAME ELEMENT

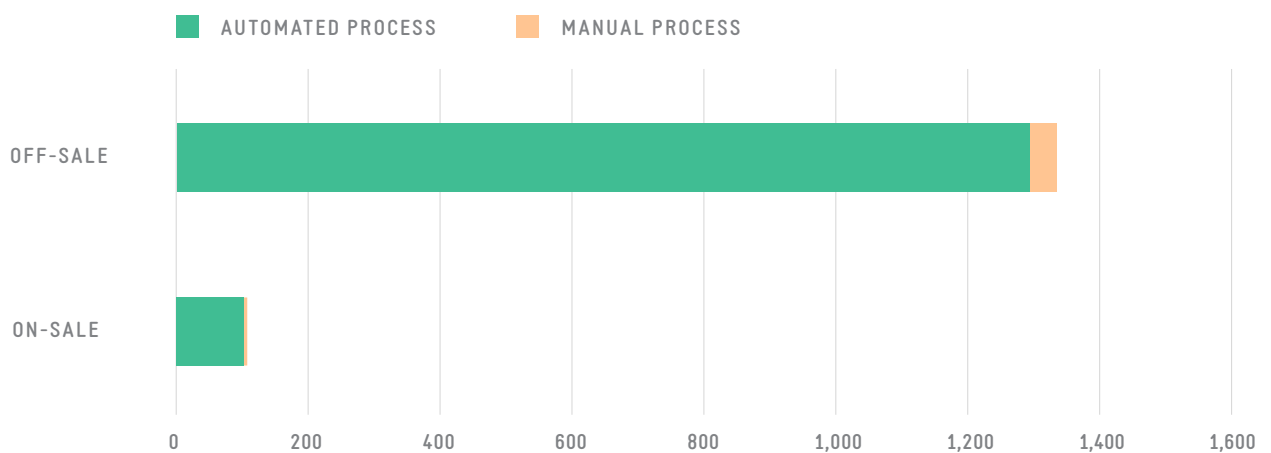
Most subscribers used automated processes for the Timeframe element of section 6.3.

- 103 out of 106 (97%) on-sale products used an automated process for the Timeframe element of section 6.3
- 1,295 out of 1,336 (97%) off-sale products used an automated process for the Timeframe element of section 6.3.

In contrast, subscribers used manual processes to meet the Timeframe element of section 6.3 for just 3 on-sale products (3%) and 41 off-sale products (3%) (Figure 3).

**FIGURE 3.**

**Process used by on-sale and off-sale products: Timeframe element**

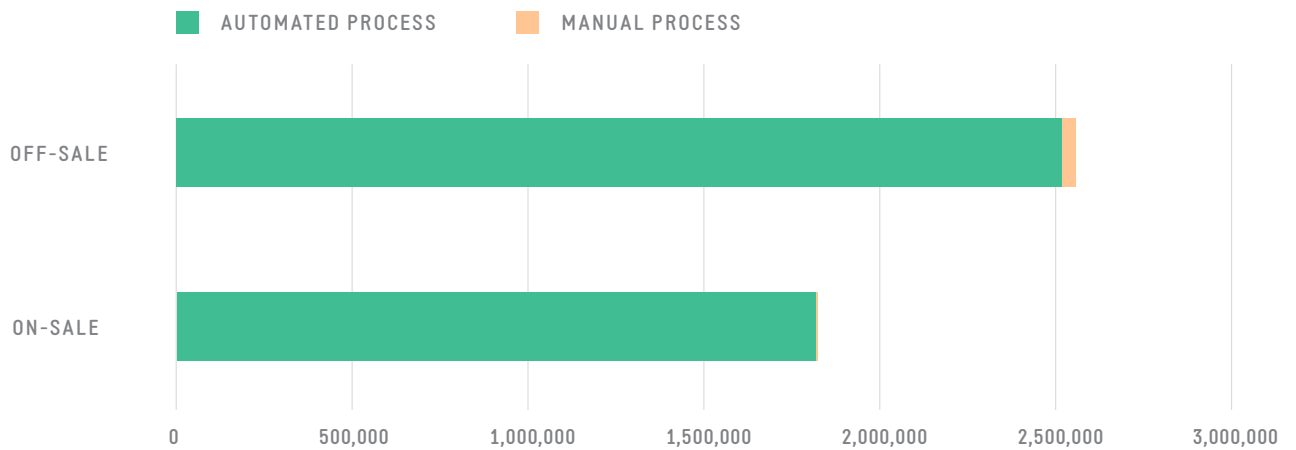


The number of customers with on-sale and off-sale products subject to a manual process for the Timeframe element was small compared to the overall number of customers covered.

- Of the 1.8m customers for all on-sale products, only 1,800 (0.1%) had active policies where subscribers used a manual process for the Timeframe element.
- Similarly, of the 2.5m customers for all off-sale products, only 37,000 (1.5%) had active policies where subscribers used a manual process for the Timeframe element (Figure 4).

FIGURE 4.

Total number of customers: Timeframe element

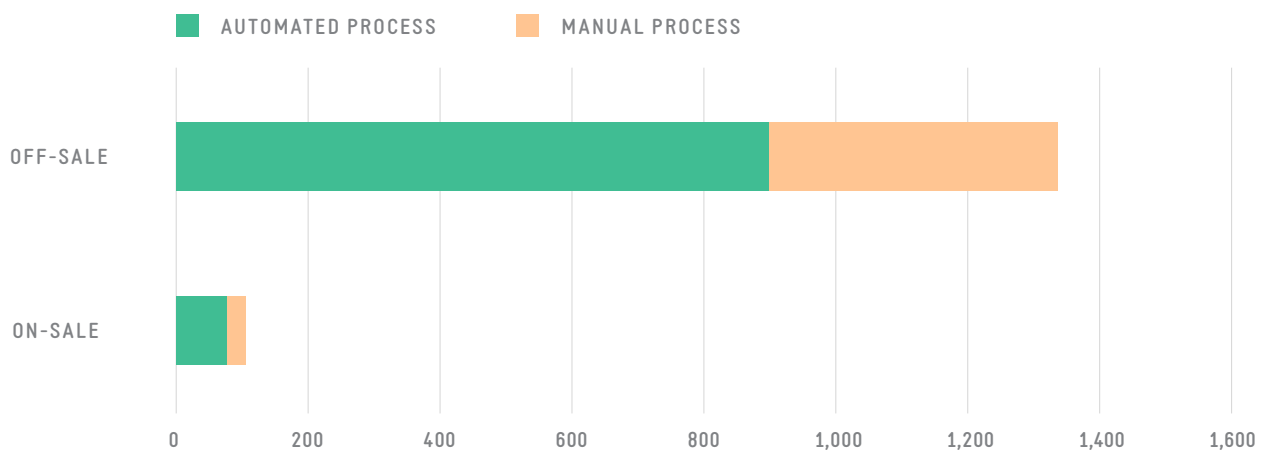


PROCESSES USED IN RELATION TO THE INFORMATION ELEMENT

Most subscribers used automated processes for the Information element. However, there were more products subject to manual processes for the Information element than there were for the Timeframe element, with 30 out of 106 (28%) on-sale products and 438 out of 1,336 (33%) off-sale products using a manual process for the Information element (Figure 5).

FIGURE 5.

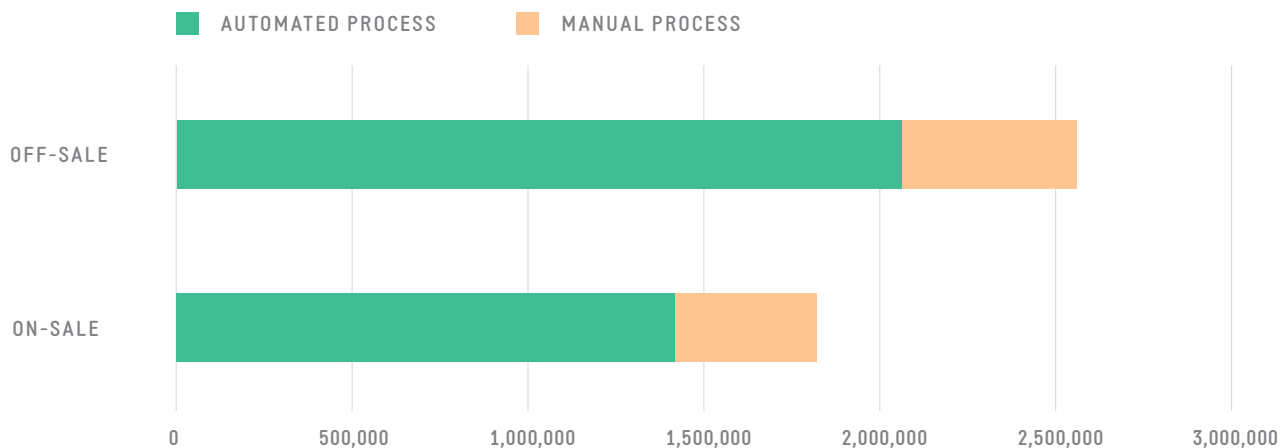
Process used by on-sale and off-sale products: Information element



The number of customers covered by a manual process for the Information element was also substantially higher for the Information element than for the Timeframe element. The 30 on-sale products covered 400,000 (22%) customers and the 438 off-sale products covered 491,000 (19%) customers (Figure 6).

**FIGURE 6.**

**Total number of customers: Information element**



## Compliance framework (Question 5)

The OMI questionnaire asked subscribers to provide information about the compliance frameworks they used to meet the section 6.3 requirements.

All subscribers, except one, provided a clear explanation of the processes and procedures they used to enable them to meet their obligations in section 6.3 of the Code.

The Committee was encouraged to note that most subscribers had built into their processes automated reminders to send an annual notice to customers 30 to 40 days prior to the anniversary of their policy. This allows subscribers sufficient time to generate and send the annual notices to customers to meet the Timeline element of section 6.3.

Subscribers mostly used automated reporting to keep track of the policies that required annual notices, and subscribers would generate a list of the relevant policies with upcoming annual notices on a regular basis. Many of the larger subscribers generated this list on a daily basis due to the large number of customers.

A significant number of subscribers relied on third party external mail-houses to send the annual notices to customers via post. In such scenarios, the Committee expects subscribers to have robust processes and Service Level Agreements (SLAs) with the external mail-houses to ensure that the annual notices are provided to customers in accordance with the timeframe in section 6.3 of the Code.

A number of subscribers also had processes that provided customers with the option of receiving the annual notice digitally, instead of via post. All subscribers that provided this option required the customer to opt-in to receive the annual notice digitally.

Most subscribers also had processes to handle mail returns and/or email bounce-backs, including reviewing the correspondence to check for errors and contacting the customer to identify the correct postal or email address. Although not a requirement of section 6.3, the Committee noted that the processes provided by subscribers did not include

safeguards to ensure that the annual notice is not sent to an incorrect address or that a customer's private information is not provided to a third party by accident.

The Committee considers it would be prudent for subscribers to conduct periodic checks of postal and email addresses for customers and have processes in place to allow customers to easily update their postal and/or email addresses. This would help to ensure that annual notices are correctly addressed and minimise the risk of inadvertent disclosure of personal information to third parties who might unwittingly access the information.

## Breach data (Question 6)

The Committee asked subscribers to provide data in relation to breaches of section 6.3 that subscribers recorded between 1 January 2019 and 31 December 2020 (the reporting period).

### NUMBER OF BREACHES

Of the 18 subscribers that provided data in the OMI, 14 subscribers reported a total of 76 breaches of section 6.3 covering multiple customers within the reporting period (Figure 7). The remaining 4 subscribers did not report any section 6.3 breaches.

FIGURE 7.

Breaches per subscriber



The 76 breaches included:

- 37 breaches in the 2019 calendar year
- 34 breaches in the 2020 calendar year
- 5 breaches occurring across both calendar years.

The majority of the breaches were concentrated within 7 subscribers:

- 7 subscribers reported 67 breaches (amounting to 88% of the total breaches reported),
- 2 subscribers reported 2 breaches each,
- 5 subscribers reported 1 breach each, and
- 4 subscribers reported no breaches.

“ The number of customers impacted by subscribers’ non-compliance with section 6.3 was similarly reflected in data collected from subscribers as part of the Committee’s annual data collection process (ADCP).

#### NUMBER OF CUSTOMERS IMPACTED

The subscribers’ 76 breaches impacted a total of 198,000 customers. More than half (114,000 or 58%) of these customers were impacted by a single significant breach by one subscriber. The other 75 breaches impacted almost 84,000 (42%) customers, with an average of 1,128 customers impacted per breach.

The number of customers impacted by subscribers’ non-compliance with section 6.3 was similarly reflected in data collected from subscribers as part of the Committee’s annual data collection process (ADCP). An initial review of breach event data received by the Committee for the 2020-2021 ADCP reporting period indicates that more than 373,000 customers were impacted by 25 section 6.3 breach events within the period. Half of the 2020-2021 ADCP’s reporting period overlapped with the OMI and indicates that subscribers have ongoing issues with section 6.3 compliance.

The subscribers’ 76 breaches impacted a total of almost

**200,000**  
customers







The data show that automated processes generated more breaches and impacted more customers per breach than manual processes.

#### BREACHES IN RELATION TO ON-SALE VS OFF-SALE PRODUCTS

Off-sale products accounted for 38 breaches, with on-sale products accounting for 24 breaches, and the remaining 14 breaches relating to a combination of on-sale and off-sale products.

The type of process used by subscribers did not impact this, with off-sale products accounting for the majority of breaches for both automated and manual processes.

Breaches relating to off-sale products were also more likely to amount to a significant breach of the Code, with 18 out of the 29 significant breaches of section 6.3 relating solely to off-sale products.

#### BREACHES IN RELATION TO AUTOMATED VS MANUAL PROCESSES

The data show that automated processes generated more breaches and impacted more customers per breach than manual processes.

65 (86%) breaches related to automated processes and impacted 82,000 (41%) customers, with an average of 1,262 customers impacted per breach.

11 (14%) breaches related to manual processes and impacted 116,000 (59%) customers, with an average of over 10,000 customers impacted per breach. However, this figure is skewed by the fact that a

single manual-process significant breach impacted 114,000 customers. Adjusting for this factor, the remaining 10 breaches relating to manual processes impacted over 2,500 customers with an average of 256 customers impacted per breach.

#### BREACHES IN RELATION TO THE TIMEFRAME ELEMENT AND INFORMATION ELEMENT

The data provided by subscribers indicated that the 76 breaches were evenly divided between the Timeframe element (35 breaches) and the Information element (31 breaches), including a small subset of breaches that related to both elements (10 breaches).

However, the 31 breaches relating to the Information element impacted far more customers (64,000 customers) than the 35 breaches relating to the Timeframe element (14,000 customers). The 10 breaches relating to both elements impacted 121,000 customers, although the Committee notes that this included the outlier significant breach with 114,000 customers impacted. Adjusting for this factor, the remaining 9 breaches relating to both the Timeframe and Information elements impacted 6,800 customers.

The 31 breaches relating to the Information element each impacted an average of over 2,000 customers, while the 35 breaches relating to the Timeframe element each impacted an average of 403 customers.



Failure to provide this information to customers on time each year prevents customers from being able to make informed choices about the suitability and affordability of policies ...

Adjusting for the one breach relating to both the Timeframe and Information elements that impacted 114,000 customers, the remaining 9 breaches relating to both elements each impacted an average of 757 customers.

According to subscribers, breaches of the Information element of section 6.3 related to issues including incorrect anniversary dates, incorrect sum insured, incorrect benefit names and incorrect product names. Failure to provide this information to customers on time each year prevents customers from being able to make informed choices about the suitability and affordability of policies, including assessing the risks of changing or cancelling a policy. It can also result in customers missing the opportunity to contact their insurer to discuss options if they wish to change their policy or are having difficulty meeting payments.



**29 of the 76 breaches reported by subscribers were deemed to be significant**

## SIGNIFICANT VS NOT SIGNIFICANT BREACHES

Of the 76 breaches reported by subscribers, 29 (38%) were deemed by subscribers to be significant and 47 (62%) were deemed by subscribers to be non-significant.

The 29 significant breaches impacted 180,000 (91%) of customers impacted by breaches, with an average of over 6,000 customers impacted per breach. Twenty-eight of the significant breaches related to automated processes and one related to manual processes.

However, a number of these significant breaches have yet to be reported to the Committee as a significant breach of the Code. The Committee encourages subscribers to refer to its Guidance Note on the significant breach obligations<sup>4</sup> that apply to subscribers and to review whether the subscriber has appropriately identified and reported all significant breaches of the Code.

The 47 breaches deemed by subscribers to be non-significant impacted 19,000 customers, with an average of 400 customers impacted per breach. Six of the non-significant breaches impacted more than 500 customers, with one non-significant breach impacting more than 12,000 customers. If the 6 non-significant breaches which each impacted more than 500 customers are excluded from the total, the average number of customers impacted per non-significant breach drops from 400 to 24.

Irrespective of the number of customers impacted by a breach of section 6.3, the potential impact on individual customers can be significant. For example, a breach of the Timeframe element can result in the customer not receiving the notice before the renewal date. If a customer has

<sup>4</sup> [https://lifeccc.org.au/app/uploads/2021/09/LCCC\\_Guidance-Note.7\\_Significant-Breach-Obligations.pdf](https://lifeccc.org.au/app/uploads/2021/09/LCCC_Guidance-Note.7_Significant-Breach-Obligations.pdf)

not set up a direct debit or a direct debit is incorrect or has been changed, their policy might inadvertently lapse. A breach of the Timeframe and/or Information element can have a significant impact on a customer who cannot afford the premium, as they might miss the prompt of contacting the insurer to discuss or consider whether the policy is still suitable or if they are having difficulty meeting their payments.

### REASONS FOR THE BREACHES

As part of the OMI, subscribers provided qualitative data on the reasons for the breaches. We have reviewed the data and classified the reasons for breaches into 3 categories:

- **Human error** – the breach related to an error by a staff member of the subscriber
- **System issue** – the breach related to an unexpected system malfunction
- **Compliance processes** – the breach related to the subscriber’s management of its section 6.3 process.

The data provided by subscribers explaining why the breaches occurred varied significantly in quality. Some subscribers provided clear details about the reasons for the breach and the specific cause of the breach. Other subscribers gave vague reasons for the breach, such as ‘manual process’, ‘coding error’ and ‘tools/technology’.

Of the 76 breaches reported by subscribers:

- human error related to 18 (24%) breaches
- system issue related to 42 (55%) breaches
- compliance processes related to 16 (21%) breaches.



The 16 breaches relating to compliance processes affected the highest number of customers, impacting 170,000 (86%) of all 198,000 customers affected by all breaches...



**42** breaches related to system issue



**18** breaches related to human error



**16** breaches related to compliance processes

The 16 breaches relating to compliance processes affected the highest number of customers, impacting 170,000 (86%) of 198,000 customers affected by all breaches. The 170,000 customers impacted by compliance processes includes an outlier breach that impacted 114,000 customers. The remaining 15 breaches relating to compliance processes impacted 57,000 (29%) customers, with an average of 3,800 customers impacted per breach.

Breaches caused by systems issues impacted 26,000 (13%) customers, with an average of 629 customers impacted per breach.

Breaches caused by human error affected 1,000 (0.05%) customers, with an average of 58 customers impacted per breach.

## Communication method (Question 7)

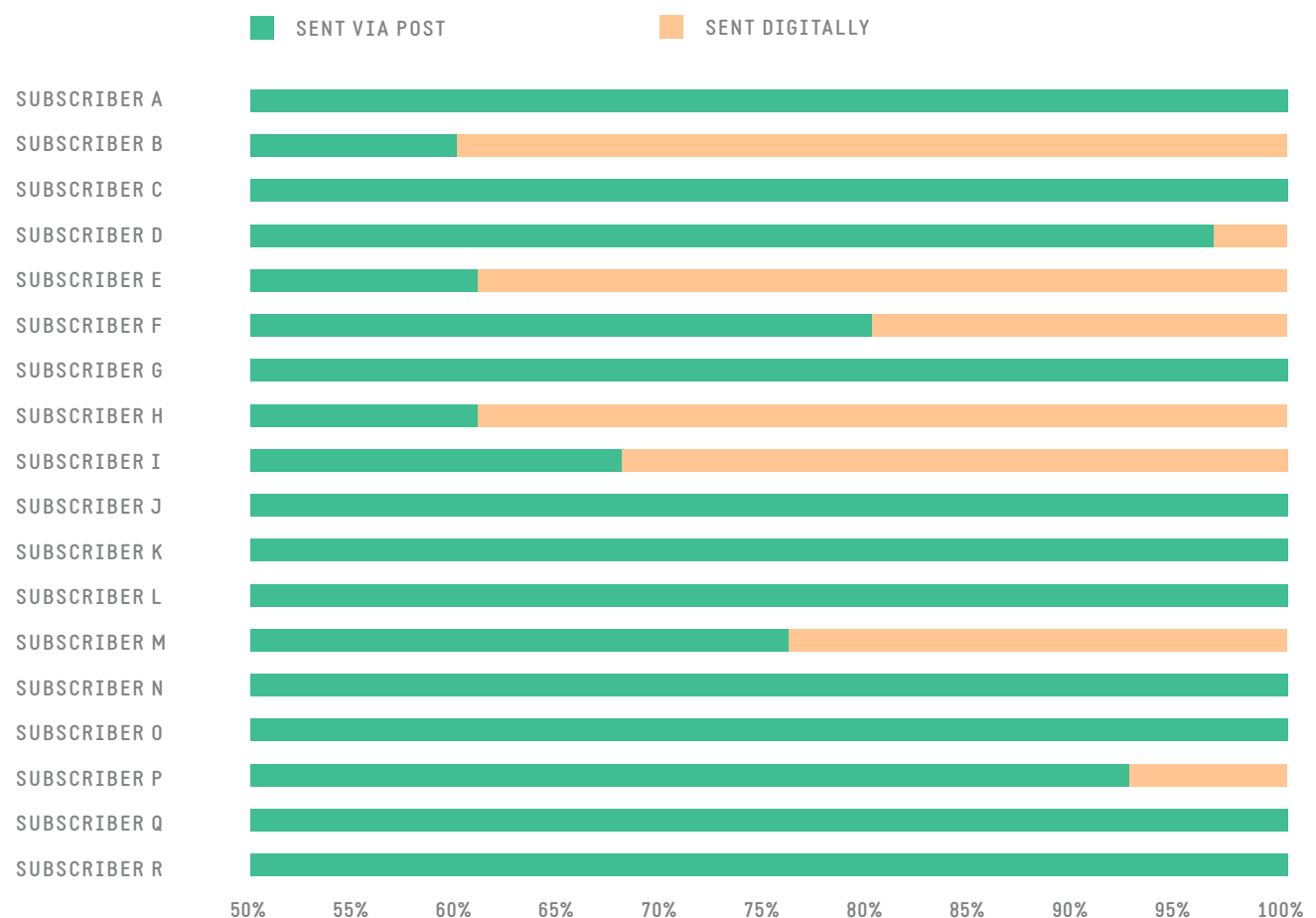
Subscribers issued 7.8m annual notices between 1 January 2019 and 31 December 2020. Subscribers issued all the annual notices either via post or digitally via email. 60% of annual notices were issued via post.

- 10 subscribers issued all their annual notices by post.
- 8 subscribers issued their annual notices by a combination of post and email.
  - › 2 subscribers issued more than 90% of their annual notices via post.
  - › 2 subscribers issued between 75% and 80% of their annual notices via post.
  - › 4 subscribers issued between 60% and 74% of their annual notices via post (Figure 8)

**7.8 million annual notices were issued by subscribers**



**FIGURE 8.**  
Percentages of annual notices sent via post vs digitally



# Observations and recommendations

## Importance of the off-sale market

Analysis of the data provided by subscribers and outlined in this report indicates that:

- There are more off-sale products on subscribers' books than on-sale products on offer.
- More customers are covered by off-sale products than on-sale products.
- More off-sale products rely on manual processes for compliance with the Information element of section 6.3 than on-sale products.
- There were more breaches, including more significant breaches, relating to off-sale products than on-sale products between 1 January 2019 and 31 December 2020.

The data raises concerns that some subscribers may have less robust systems and processes for managing compliance with section 6.3 in relation to legacy products that are off-sale. The obligations created by the Code equally protect customers of on-sale and off-sale products, and Customers of off-sale products should be provided with the same level of protection under the Code as customers of on-sale products.

Given the large number of off-sale products (13,000) and customers covered by such products (2.5m), and the number of breaches, including significant breaches of section 6.3 in relation to off-sale products, the Committee expects subscribers to have equally robust processes and procedures in relation to off-sale products as well as on-sale products.



### RECOMMENDATION 1

**The Committee recommends that subscribers review their processes for managing compliance with section 6.3 in relation to all off-sale products as well as on-sale products to ensure they remain current, accurate, robust and effective in meeting subscribers' obligations to meet both the Timeframe and Information elements of section 6.3 of the Code and to enable early detection of breaches to minimise the impact on affected customers.**

## Implementation of automated processes and monitoring and review of systems and processes

Given the large number of annual notices and customers who must receive annual notices, the Committee considers that automated processes are the most effective and efficient way for subscribers to enable compliance with section 6.3 of the Code.

Subscribers reported that 891,000 customers received annual notices through a manual process. Manual processes are still used in relation to 3% of both on-sale products and off-sale products to meet the Timeframe element of section 6.3. Manual processes are still used for 28% of on-sale and 33% of off-sale products to meet the Information element of section 6.3 of the Code.

However, automated processes do not automatically guarantee compliance with the Code. Where breaches of section 6.3 relate to automated processes, they can result in widespread impact on large number of customers. Data provided by subscribers for this OMI have identified that automated processes generated more breaches (65 of the 76 breaches, and 28 of the 29 significant breaches) and impacted more customer per breach than manual processes (1,200 customers affected per beach related to automated processes compared with 256 customers per breach related to manual processes).

Independently of this OMI, the Committee's investigations of alleged breaches of section 6.3 have identified that breaches of section 6.3 related to automated processes have sometimes occurred following mergers and changes and upgrades of systems and processes, and that they have impacted many customers. Incorporating safeguards to ensure compliance with the Code in planning and implementation of system changes and upgrades and related change management processes can assist subscribers in mitigating the risk of non-compliance with the Code and adversely impacting affected customers.

Breaches relating to the information element impacted the majority of customers. In addition, a number of subscribers reported breaches of section 6.3 in relation to a failure to properly update the templates used for the annual notices. This indicates a failure in the subscribers' monitoring of their obligations under section 6.3 of the Code.

While use of automated processes should be expected to enable compliance with section 6.3, subscribers should also be mindful that when there is a failure within an automated process, it can result in significant breaches that impact substantial numbers of customers. Subscribers should therefore ensure they have robust monitoring in place to detect any failure within an automated process so that breaches are detected as early as possible, and the number of customers impacted is minimised.



#### RECOMMENDATION 2

The Committee **recommends** that subscribers consider adopting automated processes or enhanced controls over manual processes for all on-sale and off-sale products to enable compliance with section 6.3 of the Code, in relation to both the Timeframe and the Information elements.



#### RECOMMENDATION 3

The Committee **recommends** that subscribers' planning and implementation of system changes and upgrades and related change management processes encompass checks, tests and assurances that the automated generation and issuing of annual notices complies with the Timeframe element of section 6.3 of the Code for all products.



#### RECOMMENDATION 4

The Committee **recommends** that subscribers not only monitor automated systems and processes used to ensure compliance with section 6.3 but also review the content of templates and communications used in relation to issuing annual notices to customers to ensure all the information required under section 6.3 is accurately provided to customers.

## Issuing of annual notices

Noting the potential impact on customers when subscribers breach the Timeline and/or Information elements of section 6.3, it is important that subscribers' mode of issuing annual notices is appropriate to their customers and ensures that affected customers receive their annual notices on time and with the correct information.



#### RECOMMENDATION 5

The Committee **recommends** that, irrespective of whether subscribers issue annual notices by post or digitally, they should have processes in place to maintain the currency and accuracy of all customers' postal and digital addresses, to ensure that annual notices are issued to customers in accordance with the Timeline and Information requirements of section 6.3 and to minimise the risk of inadvertent disclosure of personal information to third parties.

## Reporting of significant breaches of section 6.3

The data provided by subscribers on breaches of section 6.3 of the Code during calendar years 2019 and 2020 indicated that, despite subscribers having systems and processes to help ensure compliance with the Timeframe and Information elements of section 6.3, breaches, including significant breaches, occurred during the period. The breaches occurred in relation to on-sale and off-sale products and impacted 198,000 customers.

Since the initial section 6.3 OMI industry consultation in March 2021, subscribers have self-reported 6 significant breaches of section 6.3. In some of these significant breaches, the subscribers noted that they identified the breaches as a result of collecting and reviewing the data for the section 6.3 OMI. This demonstrates

that some subscribers are not able to continuously monitor their compliance with section 6.3 of the Code. The Committee expects all subscribers to have robust processes to identify breaches of the Code and report significant breaches to the Committee where appropriate.



#### RECOMMENDATION 6

**The Committee recommends that all subscribers ensure they have robust and effective processes to monitor compliance with section 6.3 of the Code, identify breaches and report significant breaches to the Committee where appropriate and take immediate action to notify affected customers and rectify identified breaches as quickly as possible.**

#### THIS OMI REINFORCES THE IMPORTANCE OF SUBSCRIBERS:

- ✓ Having robust monitoring in place to test and provide assurance of the accuracy, reliability and effectiveness of automated systems and processes in ensuring the Timeframe and Information elements of section 6.3 are being met
- ✓ Providing training of staff on the Timeframe and Information elements of section 6.3 and ongoing support and supervision of staff to assist them in meeting all requirements of section 6.3
- ✓ Having processes in place to detect any failure within systems and processes so that breaches are detected as early as possible and the number of customers impacted is minimised.



# Conclusion

Subscribers failing to send customers a compliant annual notice prior to the anniversary of their life insurance policy has been an area of concern for the Committee since the introduction of the Code in 2017. Compliance with section 6.3 is an important indicator of how Code subscribers prioritise transparent and timely communications with their customers. It ensures customers are aware of their policies and the details of their policies. It enables customers to make informed choices and decisions relating to the affordability and appropriateness of policies for their circumstances and to take action if they want to change their policy or are having difficulty meeting payments.



Compliance with section 6.3 is an important signifier of how Code subscribers prioritise transparent and timely communications with their customers.

The data provided by subscribers for this OMI indicates that the industry has processes and systems (mainly automated) in place to ensure compliance with the Timeframe and Information elements of section 6.3. The OMI has identified opportunities to strengthen the robustness of processes in relation to some off-sale products, extend automation of processes for generating and issuing annual notices for some on-sale and off-sale products, and put in place processes for ongoing monitoring and testing of automated processes to ensure they remain robust, reliable and effective in meeting the obligations of section 6.3, and especially following mergers, system changes and upgrades. The OMI has also identified the need for ongoing training of staff on the Timeframe and Information elements of section 6.3 and ongoing support and supervision of staff to assist them in meeting all requirements of section 6.3 and minimise the risk of breaches related to human error or weaknesses or failures in compliance processes.

# Annexure

## What is an OMI?

As the body responsible for monitoring and enforcing subscribers' compliance with the Life Code of Practice, the Life Code Compliance Committee (the Committee) utilises a variety of compliance assessment tools. An OMI is one such tool and it has the following characteristics:

- Is a targeted and focused investigation to assess how effectively subscribers are complying with a particular section or area of the Code that is considered high or emerging risk;
- Is evidence-based, proportionate and practical;
- Aims to also provide the Committee with objective insights and evidence to support subscribers' compliance with their obligations under the Code; and,
- Aims to result, where appropriate, in proposed guidance and recommendations for subscribers about how to improve service standards and compliance.

This inquiry into subscribers' compliance with section 6.3 of the Code is the Committee's second OMI since the industry's adoption of the Code in July 2017.



**Life Code Compliance Committee**  
[lifeccc.org.au](http://lifeccc.org.au)