



Insurance Council  
of Australia

Niki Del Mel  
Strategic Policy Adviser  
Australian Securities and Investments Commission  
120 Collins St  
MELBOURNE 3000 VIC Australia

[BR.submissions@asic.gov.au](mailto:BR.submissions@asic.gov.au)

June 7, 2021

Dear Ms Del Mel

### **ASIC CONSULTATION PAPER 340: BREACH REPORTING**

The Insurance Council of Australia (ICA) appreciates the opportunity to provide comments on ASIC consultation paper 340: Breach reporting and related obligations. Our members also greatly appreciated the opportunity to meet with you and your colleagues on 31 May 2021 to discuss various aspects of CP 340, and we look forward to continuing our dialogue over the coming weeks.

### **Recommendations**

Our key recommendations can be summarised as follows.

- Recommendation 1 seeks additional examples regarding the circumstances which do not involve clearly reportable conduct as they do not result in material loss or damage to clients.
- Recommendation 2 suggests additional guidance could be provided regarding how “specific financial circumstances” will in practice feed into whether material loss or damage arises.
- Recommendation 3 seeks additional examples regarding when there will be reportable “deemed significant” breaches.
- Recommendation 4 seeks additional examples to illustrate the operation of the knowledge and recklessness tests to determine when a reportable situation has arisen.
- Recommendation 5 seeks further clarity regarding what will constitute an “investigation” including through additional examples covering a range of different scenarios including smaller licensees as well as larger licensees.
- Recommendation 6 seeks further clarity regarding the application of the new breach reporting legislation to incidents that occurred prior to 1 October 2021 and remain under investigation as of 1 October 2021.
- Recommendation 7 suggests that ASIC could provide a list of core obligations in relation to what is reportable.



Insurance Council  
of Australia

- Recommendation 8 makes a number of suggestions regarding the reportable situations form that must be used to report significant breaches to ASIC.

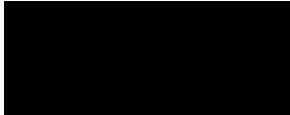
These recommendations are explained in greater detail in **Attachment A**.

We would be happy to meet with you to discuss this submission in greater detail. In the meantime, if you have any questions in relation to our submission, please contact Jongsok Oh, Senior Policy Manager, by email at [REDACTED] or on telephone on [REDACTED].

### About the ICA

The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 95 percent of private sector general insurers. As a foundational component of the Australian economy, the general insurance industry employs approximately 60,000 people, generates gross written premium of \$53.9 billion per annum and on average pays out \$166.2 million in claims each working day (\$41.5 billion per year).

Yours sincerely



Andrew Hall  
Executive Director & CEO



Insurance Council  
of Australia

## ATTACHMENT A

### DETAILED RECOMMENDATIONS

The ICA supports the ASIC proposal to include case studies and scenarios to supplement ASIC's general guidance and to help illustrate key principles as they might apply to different licensees, industries, and business models. There is a wide variety of licensees impacted by these obligations both in terms of their size and the nature and complexity of their businesses, and it is therefore important to have a level of flexibility in the application of obligations so that they can be incorporated into differing systems, processes, and operating environments. In that regard, we believe case studies specific to the general insurance industry would be of great assistance to our members.

#### Deemed significance

Reportable situations that do not require a determination of significance before being reported to ASIC include deemed significant breaches which are automatically taken to be significant by operation of law.

Deemed significant breaches that are reportable to ASIC includes breaches that result in, or are likely to result in, material loss or damage to clients. The term "material loss or damage" is not defined, although RG 78.38 notes that in determining whether there is material loss or damage, licensees should be guided by the Parliamentary intent in the explanatory memorandum (which notes among other things that whether material loss or damage arises will depend on the person's "specific financial circumstances" as explained in RG 78.39).

#### Recommendation 1

We suggest that the finalised regulatory guidance could provide additional examples about the circumstances that do not involve clearly reportable conduct as they do not result in material loss or damage to clients.

One possible example could be where a single customer was not read a general advice warning during a phone call, and this did not result in material loss or damage to that single customer, having regard to the customer's financial situation.

#### Recommendation 2

We suggest additional guidance could be provided regarding how "specific financial circumstances" will in practice feed into whether material loss or damage arises.

#### Recommendation 3

We suggest that the finalised regulatory guidance could outline whether the following scenarios would be deemed to be significant – for example, the failure to notify ASIC on time regarding a new or ceased product disclosure statements, and a failure to provide a key fact sheet.

#### Reportable situations: Knowledge and recklessness tests

As noted in RG 78.68, a licensee must report to ASIC if there are reasonable grounds to believe that a reportable situation has arisen, within 30 days after the licensee first knows of (the "knowledge" test) – or are reckless about (the "recklessness" test) – whether there are reasonable grounds to believe a reportable situation has arisen: Section 912DAA of the Corporations Act and Section 50B of



Insurance Council  
of Australia

the National Credit Act. In this regard, Example 7 in RG 78.72 provides an example of how ASIC considers the “recklessness” test to apply. RG 78.75 notes Section 769B(3) of the Corporations Act which has the effect that the “state of mind” of a “director, employee or agent” of the licensee is the “state of mind” of the licensee.

#### **Recommendation 4**

We suggest that the finalised regulatory guidance could provide additional examples to illustrate the operation of the knowledge and recklessness tests.

For example: building on Example 7 in RG 78.72 – how ASIC would treat a scenario where a licensee’s Executive Committee did not provide a directive, but the matter was not escalated to the Legal or Compliance areas?

For another example: at what point would ASIC consider “knowledge” to have arisen in Example 7 in RG 78.72? Referring to the example provided in Case Study 4 in RG 78.78 (regarding unreasonable delays due to inadequate processes), would ASIC consider knowledge to arise when a matter is escalated to the Compliance area or the relevant function that considers whether an incident is a breach?

With regard to the example of directors giving direction to not escalate issues to Compliance areas, members have noted that a more practically useful example could be around a business continuity event leading to time delays to process and investigate breaches due to resourcing constraints associated with the event.

#### **Reportable situations: investigations**

RG 78.82 notes that in the case of investigations, a licensee must lodge a report only in relation to investigations that have continued for more than 30 days.

#### **Recommendation 5**

We suggest that further clarification can be provided regarding what will constitute an “investigation” and when the investigation period is deemed to have commenced including through additional examples covering a range of different scenarios including smaller licensees as well as larger licensees. This will in our view help ensure consistency across the sector. Please see below our illustrative examples.

In that regard, members have also noted that it would be helpful to get guidance around the approach in situations where investigations are closed prior to the 30-day timeframe with the outcome ‘no breach’, but subsequently reopened with new information. Does this restart the timeframe with a new investigation or does the initial timeframe applies from the initial investigation?

The following illustrative examples have been prepared to assist ASIC in considering where an investigation might commence, particularly in relation to larger organisational structures. In our view, the questions to be considered by ASIC are:

- At what point does ASIC believe the Licensee has commenced an investigation into whether a breach or likely breach has occurred?
- At what point does ASIC believe this Licensee *first knew* that there were reasonable grounds to believe a reportable situation had arisen?



Insurance Council  
of Australia

### Example 1

A business division notices a system error which they believe has resulted in customers not receiving their insurance renewal documents. They log the incident in the licensee's Incident Management System.

The incident is escalated to a Risk team in Line 1 who make enquiries as to the details of the incident (when they think this started happening, what exactly was the system issue, how many customers do they believe may not have received their renewal documents). They also make enquiries as to whether anything has been done to immediately rectify the issue. They liaise with the relevant business division to gather these details.

Based on this information, the Risk team escalates the matter to Compliance in Line 2 for further review.

Compliance in Line 2 commences an assessment to consider whether this type of incident could result in any breach of potential laws, codes, or other applicable regulatory requirements. They also liaise with Risk and the Business to understand more of the facts around whether customers did receive their documents at all, or whether it was simply a delay. They make enquiries about the kinds of insurance products or brands that may have been impacted.

Compliance in Line 2 notifies the Legal team of the incident and asks them to consider whether, given the circumstances, there might have been any breach of financial services laws, such as the Insurance Contracts Act.

The Legal team considers the information available and determines that the business has breached its obligations under Section 58 of the Insurance Contracts Act (non-civil penalty provision). They note that the licensee may have failed to comply with its obligation to 'comply with financial services laws'. They provide this advice to Compliance and relevant Senior Management, who agree that based on that advice, the matter must be reported to ASIC.

The relevant business division prepares and lodges a report with ASIC.

### Example 2

A Quality Assurance team identifies an issue during a quarterly audit where Financial Services Guides are not being provided. They log the incident in the licensee's Incident Management System. The incident is picked up by a member of the Line 2 team during the regular incident oversight process

Compliance commences an assessment to consider whether this type of incident could result in any breach of potential laws, industry codes or other applicable regulatory requirements. They also liaise with Risk and the Business to understand more of the facts around whether customers did receive FSGs. They make enquiries about the kinds of insurance products or brands that may have been impacted.

Compliance notifies their Legal team of the incident and asks them to consider whether, given the circumstances, there might have been any breach of financial services laws such as the Corporations Act.

The Legal team considers the information available and determines that the business has breached its obligations under Section 941A of the Corporations Act. They note that the licensee may have failed to comply with its obligation to 'comply with financial services laws'. They provide this advice to Compliance and relevant Senior Management, who agree that based on that advice, the matter must be reported to ASIC.

The relevant business division prepares and lodges a report with ASIC.



Insurance Council  
of Australia

## Transitional arrangements

Our members appreciate the clarification around transitional arrangements as set out in RG 78.14 to RG 78.18 in relation to the breach reporting obligations applying to reportable situations that arise on or after 1 October 2021.

### Recommendation 6

We suggest that further clarification can be provided in relation to incidents that occurred prior to 1 October 2021 and remain under investigation as of 1 October 2021.

Specifically, will licensees need to report these matters to ASIC as matters that are under investigation (which has continued for more than 30 days)? On what date will the matter be reportable? Do all these investigations that have been open for more than 30 days become reportable on 1 October 2021 and therefore must be reported by 1 November 2021?

It would be helpful if ASIC could clarify through a case study with reference to a licensee's open incidents in its breach reporting register prior to 1 October 2021.

## Core obligations

A licensee must report to ASIC any significant breach (or likely significant breach) of its "core obligations" as defined in Section 912D (3) of the Corporations Act for Australian Financial Service (AFS) licensees.

These "core obligations" include (for AFS licensees) the general obligation under Section 912A of the Corporations Act (other than the obligation under Section 912A(1)(c) to comply with financial services laws – aside from those parts of the definition set out in Section 912D(3)(b)) and the general obligations under Section 912B of the Corporations Act.

### Recommendation 7

We suggest that ASIC could provide a list of core obligations in relation to what is reportable. It would in our view significantly assist in ensuring a consistent approach across the financial services sector particularly in relation to smaller licensees. We also suggest further clarity on how the breach reporting requirements might interact with the enforceable code provisions.

## Reportable situation form

RG 78.86 notes that a licensee must report to ASIC using the prescribed reportable situation form through the ASIC regulatory portal (with Table 8 providing an overview of the content of the reportable situation form).

### Recommendation 8

We suggest that ASIC could expressly state whether all the fields are mandatory, noting that the relevant information may not always be available at the time of reporting. We would also appreciate clarification on whether: the prescribed form will replace the existing form on the ASIC regulatory portal; updates will be submitted via the regulatory portal (And if so whether there will be a separate form required); and ASIC expectations on the frequency of updates.