INSURANCE COUNCIL OF AUSTRALIA

19 May 2017

ASIC Enforcement Review
Financial System Division
The Treasury
Langton Crescent
PARKES ACT 2600

By email: ASICenforcementreview@treasury.gov.au

Dear Sir/Madam

Self-reporting of Contraventions by Financial Services and Credit Licensees

The Insurance Council of Australia (the Insurance Council) welcomes the opportunity to comment on the Treasury's Position and Consultation Paper 1, *Self-reporting of contraventions by financial services and credit licensees* (the Consultation Paper), as part of its ASIC Enforcement Review. The Insurance Council supports enhancements to the breach reporting obligations to improve the effectiveness of self-reporting in the regulatory regime, in particular, any measure which improves transparency and promotes simplicity.

The key to an effective self-reporting regime is that it strikes an appropriate balance; providing the regulator with notification of matters of which it should be aware without resulting in the reporting of every minor contravention. Whilst we acknowledge the concerns raised in the Consultation Paper about delays in reporting caused by the need for a high degree of certainty that a breach has occurred, lowering the reporting threshold too far will substantially increase the volume of reporting. This would not only have an impact on the compliance burden for reporting entities, but also obscure the more significant reports that warrant regulatory focus.

While the Insurance Council is supportive in-principle of several positions put forward in the Consultation Paper, we caution against any changes that would increase ambiguity in the current reporting regime. From the perspective of Australian Financial Services (AFS) licensees, modifying the current reporting obligation by inserting a "reasonable person" test would result in increased uncertainty.

The Insurance Council also suggests that when a Regulatory Impact Analysis (RIA) is conducted in the future, it consider the additional costs which the industry will bear as a consequence of the industry funding of ASIC.

The Attachment to this submission only comments on the positions put forward in the Consultation Paper that are relevant to the general insurance industry.

Insurance Council of Australia Limited ABN 50 005 617 318
PO Box R1832 Royal Exchange NSW Australia 1225
t +61 2 9253 5100 f +61 2 9253 5111
www.insurancecouncil.com.au

If you have any questions or comments in relation to our submission, please contact John Anning, the Insurance Council's General Manager Policy, Regulation Directorate, on (02) 9253 5121 or janning@insurancecouncil.com.au.

Yours sincerely

Robert Whelan
Executive Director and CEO

INSURANCE COUNCIL OF AUSTRALIA

ATTACHMENT

1. Position 1: The "significance test"

The Insurance Council agrees in-principle with the retention of the significance test in Section *912D of the Corporations Act 2001* (Cth) (the Corporations Act) with a materiality threshold for reporting. We are concerned however that the inclusion of the additional "reasonable person" test will not provide the requisite objective certainty members require to improve significant breach disclosure to ASIC.

Our members' experience with the "reasonable person" test is that it is most effective in circumstances where both (a) the cause being determined and (b) the effect being measured are non-complex in nature. Effective examples of the "reasonable person" test can be found in the:

i) continuous disclosure provisions of the Corporations Act; and

ii) Notifiable Data Breaches scheme under the new *Privacy Act 1988* (Cth).

In contrast, when applying the "reasonable person" test to the factors set out in subsection 912D(1)(b), questions arise as to whether licensees should consider significance from their own perspective, the regulator's or consumers'. We note that what a "reasonable person" considers to be significant is a substantially different test to what the regulator considers to be significant under the Financial Conduct Authority (FCA) requirements.

The following scenario demonstrates how slight variances to the same factual scenario can have a materially different outcome when the "reasonable person" test is applied.

Scenario

A licensee who has recently commenced trading failed to send a Product Disclosure Statement to 100 customers.

- Small Licensee
  - The 100 customers impacted represented the licensee's entire portfolio.
  - It is foreseeable that a "reasonable person" would consider that a significant breach had occurred irrespective of any remedial action undertaken.
- Medium Licensee
  - The 100 customers impacted represented less than 10% of the licensee's portfolio.
  - In this case, it is less clear whether the breach would be considered significant by a "reasonable person", assuming that timely remedial action had been undertaken by the licensee.
- Large Licensee
  - The 100 customers impacted represented less than 1% of the licensee's portfolio.
  - In this case, it is unlikely that a "reasonable person" would consider the breach significant, assuming that timely remedial action had been undertaken by the licensee.

Insurance Council of Australia Limited ABN 50 005 617 318
PO Box R1832 Royal Exchange NSW Australia 1225
t +61 2 9253 5100 f +61 2 9253 5111
www.insurancecouncil.com.au

An example of where a "reasonable person" test has been problematic is section 21(1) of the *Insurance Contracts Act 1984* (Cth). This section applies a "reasonable person in the circumstances" test which has resulted in conflicting judicial decisions and the need for subsequent legislative reform.

The Insurance Council suggests that, rather than legislating the "reasonable person" test, a more effective and less ambiguous regulatory regime could be achieved through an expansion of ASIC guidance measures. Examples include:

- expanding Regulatory Guide 78 - *Breach reporting by AFS licensees* to include objective metrics for licensees to utilise. The benefit of expanding ASIC guidance, as opposed to amending the legislative obligation, is that objective measures can be better tailored to specific products or markets and provide greater flexibility to reflect any required changes to metrics over time.
- including in Regulatory Guide 78 - *Breach reporting by AFS licensees* a comprehensive range of examples of what ASIC consider to be a 'significant breach'.
- developing a de-identified database of information outlining the types of breaches that have been disclosed to ASIC, the circumstances of the breach, the remedial action taken (if any) by the licensee, ASIC's view on whether a breach occurred or not and the penalty issued (if any). The database should be made accessible to licensees who could then consider it as a guide to how ASIC may approach the breach once notified.
- establishing an anonymous ASIC hotline where licensees could seek guidance on whether a breach has occurred without disclosing their organisation's details.

However, the Insurance Council submits that ASIC guidance can only be given within the parameters of the governing legislation and not negate its policy intent. The Consultation Paper suggests that ASIC guidance could supplement the legislative obligation by specifying breaches that should always be reported i.e. any breach of the provisions provided as examples under paragraph 29 would be deemed significant. This would in effect negate the materiality threshold in the legislation and potentially result in the reporting of numerous minor contraventions, undermining the objective of ensuring ASIC's resources are utilised efficiently and minimising the compliance burden on industry.

For example, subsection 949A(5)(5) requires a financial services licensee to take reasonable steps to ensure that an authorised representative of the licensee complies with the obligation to give a general advice warning. A failure can result in 200 penalty units or imprisonment for 5 years, or both. What are "reasonable steps" can be open to argument, and often breaches of this obligation would not normally meet the significance test for the purposes of breach reporting. An example would be a one off breach by one authorised representative due to an unintentional omission by the licensee to provide them with a document containing the notice (due to a misprint or other unintentional unusual circumstance).

The Insurance Council recommends that, as part of its ASIC Enforcement Review, Treasury works with ASIC and industry to consider the implications for legislative parameters in the areas where ASIC guidance will be expanded.

2. Position 2: Breaches by employees/representatives

The Insurance Council in principle supports change that would improve accountability in the financial services sector and streamline the regulatory relationship between ASIC and licensees. It is critical however that any amendments made to the current regulatory reporting regime strike the appropriate balance to ensure that neither under disclosure nor over disclosure of breaches to ASIC occurs.

If a licensee's obligation to report significant breaches were extended to include the conduct of employees and representatives, the following consequences are likely:

(i) a substantial growth in the number of misconduct or significant breach reports to ASIC;

(ii) an increase in resources required by insurers to monitor, investigate and disclose potential and actual significant breaches; and

(iii) an increase in resources required by ASIC to review significant breach disclosures, investigate, penalise and where necessary seek Court intervention.

Thought needs to be given to how this extended obligation will interact with the proposed expansion of reporting (i.e. "*may have or may occur*") to ensure that the reporting of suspected breaches does not have an impact on the procedural fairness accorded to affected employees/representatives. We note that specific guidance material would also be required from ASIC to outline the circumstances when breaches relating to the conduct of an employee will need to be reported, particularly in relation to the conduct of junior employees.

Consistent with the reporting of licensee breaches, the materiality threshold should also apply to the reporting of breaches by an employee or representative. While this is reflected in Position 2, it is not clear that the significance test is also proposed to apply to reporting triggered by section 920A. The Consultation Paper (paragraph 28) suggests that matters referred to in section 920A which might be appropriate for licensees to report include where the licensee has reason to believe or suspect that an employee or authorised representative:

- has become an insolvent under administration; or
- has engaged in fraudulent conduct; or
- is not of good fame and character; or
- is not adequately trained or is not competent to provide a financial service or financial services.

Particularly in relation to the adequacy of training or competence of an employee/representative, not applying the significance test could result in breach reporting being triggered by minor contraventions, such as isolated instances of failure to follow procedures.

Finally, the Insurance Council recommends that when the RIA is conducted, consideration be given as to how this extension impacts upon directors' and officers' liability.

3. Position 3: When a breach is to be reported

One of the primary issues with the current breach reporting regime is the ambiguity surrounding when the 10 day time frame to report a significant breach to ASIC commences. The Insurance Council agrees with the Consultation Paper position that this issue is largely because of subjective factors surrounding when a licensee becomes aware of the breach and whether the breach is significant. The Insurance Council submits that the appropriateness of the proposed changes under Position 3, to a large extent, will be dependent on the effectiveness of the reforms under Positions 1 and 2 to clarify the reporting thresholds.

The expansion of the reporting obligation to include breaches that "*may occur"* introduces an element of subjectivity which should be avoided. The inclusion of these words creates the potential for a large number of unnecessary disclosures to be made to ASIC where a future breach *may* occur, but due to appropriate risk mitigation measures by a licensee, is avoided entirely. Our members suggest that an alternate approach is for a licensee to make a report to ASIC within 10 business days when "the licensee becomes aware or has reason to suspect that a breach has occurred, may have occurred *or will occur* in the future". This ensures that only unavoidable future breaches are disclosed to ASIC.

The Consultation Paper suggests that a licensee could be deemed to be aware of the facts and circumstances that established the breach where the licensee has received that information from:

- a government agency;
- its auditor;
- an industry Ombudsman, or other body to which the licensee must belong under its external dispute resolution scheme obligations; and/or
- a current or former representative or employee who has provided it to a director, secretary, or senior manager of the licensee or a person authorised by the licensee to receive whistle-blower type disclosures.

There needs to be clarity around how such information will impact the consideration of the materiality of a breach. It is also unclear whether deeming awareness implies licensees should assume such information to always be correct, despite having a contrary view.

The Consultation Paper queries whether the 10 business day period to be retained for reporting of actual or suspected breaches is appropriate. The Insurance Council submits that this reporting period remains appropriate, however that the mechanisms governing the timeframe could be enhanced. Our members support a disclosure process which is comprised of:

(i) *Short form notification* – an electronic prescribed form which notifies ASIC when the licensee has discovered a suspected breach (or unavoidable future breach) and that investigations have commenced. Short form notification would need to include details of the suspected breach and details of when investigations are likely to be finalised. Ideally, this notification would be condensed into a 'tick-a-box' style form. The focus of this form is prompt ASIC notification, rather than substantive detail.

(ii) *Substantive notification* – following short form notification to ASIC and after the licensee has finalised its internal investigations, a briefing should occur between the licensee and ASIC to discuss the breach, remediation and any further action required. Substantive notification should occur as soon as practicable following short form notification, but would not be required if the licensee subsequently determined that a significant breach had not occurred.

Our members believe that 10 business days would be sufficient to comply with a short form notification to ASIC. However, 10 business days would be insufficient for large licensees to undertake appropriate investigations across multiple business levels, determine whether a breach is significant and disclose it to ASIC.

The Consultation Paper also queries whether the threshold should be extended, as it has in the United Kingdom, to broader circumstances such as where a licensee "has information that reasonably suggests" a breach has or may have occurred. As with the words "*or may occur"* discussed above, this proposal has the potential to markedly increase the number of significant breach disclosures made to ASIC, akin to levels which existed in Australia prior to 2003. Our members do not support the expansion of the threshold in this manner as:

- licensees will become overburdened with regulatory disclosure;
- there will be considerable cost implications for licensees as a result of an increase in resources required to monitor, investigate and disclose potential and actual breaches; and
- considerable strain will be placed on ASIC resources, possibly to the point where data collected is never reviewed.

4. Positions 4, 5 and 6: Penalties

The Insurance Council agrees that for ASIC to fulfil its statutory functions it must have appropriate regulatory powers to deter and penalise non-compliance. Our members believe that the current maximum prison term and monetary penalties are adequate. We highlight however that non-compliance exists in different forms and that penalties for non-compliance should be weighted towards the gravity of the offence after taking into consideration the impact on consumers.

Presently, no distinction exists between the various forms of non-compliance which occur. Our members support the breach reporting penalty regime being split into a tiered system where the penalties for simple non-compliance are less severe than those that exist for deliberate non-compliance.

The Insurance Council believes that there is merit in evolving the current regulatory penalty scheme to one that comprises:

(i) licensee level infringement notices (for minor/simple non-compliance);

(ii) licensee level civil penalties (for major non-compliance); and

(iii) imprisonment and/or criminal fines (for deliberate and severe non-compliance) of individuals and licensees.

Such a scheme would encourage licensees to be more transparent with ASIC, particularly if they knew in advance the type of penalty that the regulatory breach was likely to result in. Accordingly, the Insurance Council recommends that if a tiered penalty scheme were developed, it should be supported with robust guidelines which outline the type of offence each penalty tier is likely to attract.

5. Position 7: Cooperative approach

The Insurance Council agrees in-principle with the inclusion of provisions that encourage a more collaborative approach between licensees and ASIC. Strict enforcement of the law is at times appropriate and necessary. However, for mature markets like general insurance where licensees have a good record of compliance, a more cooperative and outcomes focused approach to supervision can be more productive.

The Consultation Paper suggests that an additional option may be to allow ASIC to take no administrative or civil action against the licensee if the licensee cooperates with ASIC and addresses the matter to ASIC's satisfaction. The Insurance Council recommends specific criteria be established to ensure consistency and fairness in ASIC's approach.

Within the context of self-reporting, the Insurance Council suggests that ASIC should consider establishing a mechanism to enable licensees to seek guidance on an anonymous basis. The Insurance Council's members have had positive experiences with such mechanisms established by the Office of the Australian Information Commissioner (OAIC) and the Australian Transaction Reports and Analysis Centre (AUSTRAC).

6. Position 8: Prescribed reporting content

The Insurance Council agrees in-principle with the prescribing of content of reports under section 912D and requiring reports to be delivered electronically. This would assist compliance processes by reducing the likelihood of ASIC seeking further information. To ensure that the reporting process is as efficient as possible (in respect of both actual and suspected breaches) the Insurance Council recommends that any prescribed reporting be consistent with the recommendations contained at Position 3 of this submission and content development should be subject to consultation with industry.

7. Position 10: Qualified privilege

The Insurance Council supports the proposed review of section 1100A of the Corporations Act to ensure qualified privilege continues to be provided to AFS licensees if the proposed reforms to breach reporting were to proceed. This is particularly critical if licensees are expected to report suspected breaches.

8. Position 12: Publication of breaches

The Insurance Council supports the retention of ASIC's current aggregate level data reporting. Moving towards a system which reports at a licensee level is not supported by our members as it will have the following consequences:

(i) Licensees who have a strong reporting culture and processes will be punished for making frequent reports to ASIC. A 'user pays' ASIC funding model will compound this issue further.

(ii) Licensees who operate multiple businesses under a single licence will be penalised as the level of breaches attributable to that licensee will be disproportionate to their smaller licensee counterparts, giving the impression to consumers that their approach to compliance is below the required standard.

(iii) The practical outcome of naming licensees who breach their regulatory requirements is that it may potentially discourage the culture of openness, honesty and transparency which ASIC seeks to develop with licensees.

(iv) Data will not compare 'apples with apples' given that the size of licensees in the market varies considerably. Consequently, reporting will not take into consideration market share or concentration meaning that data is liable to be misinterpreted by anyone outside of the financial services industry potentially resulting in reputational damage.

If, however a decision is made following this review to proceed with licensee level reporting, the threshold for disclosure should be one of exception, attracting only the most extreme breaches. For example, ASIC should only report on:

(i) deliberate avoidance of mandatory breach reporting by a licensee;

(ii) recurrent and systemic licensee breaches where ASIC remediation orders were not complied with;

(iii) deliberate conduct which resulted in a significant customer detriment; and

(iv) criminal misconduct.

Reserving licensee level reporting for the most extreme cases lowers the potential reputational damage on licensees whilst still encouraging a culture of openness, honesty and transparency with ASIC.