INSURANCE COUNCIL OF AUSTRALIA

Mr Richard Glenn
Assistant Secretary
Business and Information Law Branch
Attorney-General's Department
4 National Circuit
BARTON ACT 2600

30 November 2012

Via email: Privacy.Consultation@ag.gov.au

Dear Mr Glenn

DISCUSSION PAPER: AUSTRALIAN PRIVACY BREACH NOTIFICATION

The Insurance Council of Australia (the Insurance Council) welcomes the opportunity to provide a submission to the Attorney General's Department (AGD) consultation on *Australian Privacy Breach Notification* (Discussion Paper).

Insurance Council members take their privacy obligations very seriously and collect, use and disclose a significant amount of personal (names, addresses) and sensitive (health details) information in the course of providing quotes, issuing policies, and paying insurance claims.

This strong commitment to best practice is reflected in the consistently very low level of general insurance privacy complaints to the Commissioner in comparison to the 31 million retail policies in force in 2010-11, with the Office of Australian Information Commissioner's (OAIC) 2010-2011 Annual Report listing 35 complaints for both life and general insurers (page 31). (No category for insurance complaints appeared in the 2011-12 report.) The general insurance industry has invested significantly in secure systems and training to foster a culture of best practice in relation to the OAIC's Guide to Handling Personal Information Security Breaches (Guidance).

The Insurance Council suggests that the 27% increase outlined in the Discussion Paper for privacy notifications generally in the last year illustrates the effectiveness and increasing awareness overall of the Guidance by organisations.

From the perspective of the general insurance industry, with general conformity by members to the Guidance, the Insurance Council's preference is for the AGD to continue to build on awareness of the Guidance. However, if in order to encourage greater privacy protection across the economy, a decision is taken to introduce mandatory breach notification provisions, the Insurance Council considers that the existing Guidance could provide a possible regulatory model for future consultation purposes.

Our responses to the Discussion Paper questions are outlined in **Attachment A**. If you require further information, please contact Mr John Anning, Insurance Council's General Manager Policy- Regulation Directorate at janning@insurancecouncil.com.au.

Yours sincerely

Robert Whelan
Executive Director & CEO

INSURANCE COUNCIL OF AUSTRALIA

ATTACHMENT A

Issue 1: Should Australia introduce a mandatory data breach notification law?

- *Are the current voluntary data breach notification arrangements sufficient?*
- *Should the Government introduce a mandatory data breach notification law?*

Industry response:
For the reasons outlined in the Discussion Paper, the Insurance Council submits the existing arrangements and voluntary Guidance for breach notification are sufficient and introduction of a mandatory breach notification is unnecessary.

The voluntary arrangements provide adequate flexibility in considering the materiality of the breach, and if retained, would minimise systems and training costs within organisations at a time when future training relating to enhancements to the Privacy Act will be required. The intention that mandatory notification would capture "a real risk of serious harm" breaches is adequately addressed by the existing National (and newly legislated Australian) Privacy Principles and the Guidance which strongly encourages notification for such breaches. Any failure by an organisation to notify could be addressed by the OAIC using its existing powers.

If further changes to privacy laws for notification purposes are made, the Insurance Council submits consideration should be given to aligning commencement dates[1] to provide sufficient time to comply and provide efficiency of staff training and updates to systems and manuals.

Issue 2: Which breaches should be reported?

- *What should be the appropriate test to determine the trigger for notification?*
- *Should it be based on a 'catch all' test, or based on more specific triggers, or another test?*
- *What specific elements should be included in the notification trigger?*

Industry response:
As noted above, the Insurance Council's preference is that the voluntary notification Guidance continue. However, should a decision be taken by the Government to require mandatory notification, the Insurance Council submits that the Guidance could be used as the framework for the mandatory notification process. The Guidance sets out at page 17:

> *In general, if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified.*

The Guidance also takes into account flexibility and circumstances when notification may not be appropriate:

> *While notification is an important mitigation strategy, it will not always be the appropriate response to a breach. Providing notification about low risk breaches*

[1] The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 provides a 15 month transition. A government review is anticipated 12 months from commencement. The commencement date of notification requirements should take into account these transition and evaluation periods.

can cause undue anxiety and de-sensitise individuals to notice. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

The proposed Canadian approach in the Discussion Paper offers a similar and useful approach to breach notification. In that case, the organisation determines whether notification to affected individuals is triggered where it is reasonable, in the circumstances, to believe that the breach creates a real risk of significant harm. If so, notification is to take place as soon as feasible. It is noted the Canadian Bill does not propose penalty provisions in relation to notification requirements.

Issue 3: Who should decide on whether to notify?

- *Who should be notified about the breach?*
- *Which of the below should decide whether to notify?*
  (i) the organisation or agency;
  (ii) the Commissioner; or
  (iii) the organisation/agency in consultation with the Commissioner.

Industry response:
The Insurance Council submits the organisation, which has the direct relationship with the individual, should notify the individual(s) where a real risk of serious harm has been identified. The organisation is best placed to consider the facts and circumstances of the breach and conduct a risk assessment of its potential harm. This approach is consistent with the existing Guidance and could avoid potential delays caused by an external agency, or the Commissioner, being required to separately consider the breach notification issue. If an external agency or the Commissioner were to decide on notification, adequate resourcing would most probably be necessary in order to avoid delays.

The Commissioner may have a role to play however in this sense: If a data security breach results in a real risk of serious harm the OAIC should be notified as set out in the Guidance. Any failure by an organisation to notify could be addressed by the OAIC using its existing powers.

Issue 4: What should be reported (content and method of notification), and in what time frame?

- *What should be the form or medium in which the data breach notification is provided?*
- *Should there be a set time limit for notification or a test based on notifying as soon as is practicable or reasonable?*
- *What should be the content of the notification?*

Industry response:
The Insurance Council submits the Guidance already appropriately considers the form, medium and timing of notification. The Insurance Council considers that sufficient flexibility to take into account the particular circumstances of the breach is necessary.

The Guidance sets out that notification of individuals affected by the breach should occur as soon as reasonably possible. As discussed above, the Insurance Council considers the

Canadian approach “as soon as feasible” or as soon as “practicable in the circumstances” would also be appropriate.

Issue 5: What should be the penalty for failing to notify when required to do so?

- *Should there be a penalty or sanction for failing to comply with a legislative requirement to notify?*
- *If so, what should be the penalty or sanction, and the appropriate level of that penalty or sanction?*

Industry response:
If a decision is taken to introduce a mandatory notification requirement, the Insurance Council submits that the damage to an organisation’s reputation in not notifying a serious breach is likely sufficient incentive for compliance. However, if a penalty is to apply we submit the new penalty provisions of the Privacy Act in relation to serious or repeated breaches should be sufficient to apply to a failure to notify where a breach creates a real risk of serious harm to the individual. An additional penalty is therefore not considered necessary. It is also noted that the proposed Canadian Bill does not contain a penalty for failure to notify.

Issue 6: Who should be subject to a mandatory data breach notification law?

- *Who should be subject to a mandatory data breach notification law?*
- *Should the scope of a mandatory data breach notification law be the same as the existing scope of the Privacy Act?*

Industry response:
If a decision is taken to introduce a mandatory notification requirement, the Insurance Council supports the ALRC recommendation that the requirement apply to all entities regulated by the Privacy Act so that the scope is the same as the Privacy Act.

Issue 7: Should there be an exception for law enforcement activities?

- *Should there be an exception for law enforcement activities?*
- *Would such an exception add anything to the ALRC’s proposed public interest exception?*

Industry response:
Not relevant to the Insurance Council.