Law Council
OF AUSTRALIA
Business Law Section

Mr Timothy Pilgrim
Privacy Commissioner
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001
Via email: consultation@oaic.gov.au

4 December 2015

Dear Mr Pilgrim

OAIC consultation on developing a data breach response plan

Thank you for the opportunity to provide feedback in the above plan.

The Privacy Law Committee of the Business Law Section of the Law Council of Australia ('the Committee') has structured its feedback in response to the stimulus questions in the form of a table below.

The Committee notes that on 3 December 2015, the Government commenced consultation on a mandatory data breach regime. The Committee's feedback is focused exclusively on a data breach response that is voluntary.

Question	Feedback	Other recommendations
Is the draft guide helpful and easy to read?	Yes. The illustrations at "Responding to a large scale data breach: An illustration of how to work through the Four Key Steps' are particularly helpful.	The draft guide proceeds on the basis that there is no mandatory data breach notification requirement. It would be helpful to expressly state that. Similarly, it would assist if the OIAC could articulate examples that the OAIC considers 'real risk of serious harm' and what is the given time frame for this assessment.

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

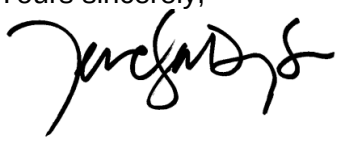
Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

BLS

Does the draft guide provide adequate assistance for entities to develop a data breach response plan?	The draft guide is useful for larger organisations or organisations that work in heavily regulated industries. Typically, such organisations have developed compliance processes and are supported by staff with expertise in the area. However, smaller organisations may need a simpler versions of the guide or a clear statement that for some organisation the absence of an articulated plan is not a bar to compliance with the *Privacy Act 1988* and a failure to take reasonable steps as required by the Act. For example, in some cases is it sufficient to deal with data breach as part of the organisation's privacy policy?	It would be helpful to articulate what the effect of the notification to the OIAC and the individual would be. For, example is the act of notification a defence (in whole or in part) for some or all types of breaches. How does this impact on systemic issues and their ongoing management?
Does the draft guide accurately and appropriately complement the OAIC's DBN Guide?	Yes	
When the DBN guide is next updated, the OAIC is considering incorporating the draft guide into the DBN Guide. Is there merit in keeping the draft guide as a stand-alone document or should the OAIC incorporate the draft guide into a revised version of the DBN guide?	There is merit in the DBN guide being a standalone document. This would assist with clarity and brevity. Should mandatory data breach notification legislation be passed, the stand alone document could easily be updated and continue to be useful by supporting compliance with the mandatory requirements.	
Are there any other ways in which the draft guide could be enhanced?	It would be helpful to articulate some industry research or other evidence articulating that voluntary disclosure promotes transparency and trust in the organisation or agency.	We note that this argument is based on the voluntary nature of the notification and the discretion exercised by the given organisation in the given circumstances. This position would be eroded by the introduction of a mandatory legal duty or requirement. To the extent that DBN Guide is a precursor to a mandatory regime the status of the OIAC recommendation or guidance will need to be adequately articulated and if need be updated.

If you have any questions in relation to these comments, in the first instance please contact the Committee Chair, Olga Ganopolsky, on 02-8237 9194 or via email: olga.ganopolsky@macquarie.com

Yours sincerely,



Teresa Dyson, Chairman
Business Law Section