Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Department of Finance
Contact details *(one or all of the following: postal address, email address or phone number)*	Patricia Hawley Assistant Secretary Legal Services Branch [contact details redacted]

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? NO

Your submission

The Department of Finance (Finance) makes the following comments in relation to the draft Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill).

The Bill was developed in response to the Australian Law Reform Commission's 2008 report *For Your Information: Australian Privacy Law and Practice* (ALRC report) which described mandatory data breach notification as, *'in essence, a legal requirement on agencies and organisations to notify individuals when a breach of security leads to the disclosure of personal information'*.

Finance notes that the ALRC report refers to a legal requirement on agencies and organisations to notify individuals of a serious data breach but does not necessarily refer to a legal requirement to notify the Office of the Australian Information Commission (OAIC) of a serious data breach.

Finance agrees that there is a strong rationale for requiring agencies and organisations to notify individuals of a serious data breach. In particular, the ALRC report noted that such a notification would allow individuals whose personal information has been compromised in a data breach to take remedial steps to avoid potential adverse consequences, such as financial loss or identify theft.

However, it is not clear to Finance that there is a strong rationale for requiring agencies and organisation to notify the OAIC in all cases of a serious data breach. A data breach will be considered a serious data breach where there is a real risk of serious harm to the individual. Serious harm, includes physical, psychological, economic and financial harm, as well as harm to reputation. Paragraph 8 of the Explanatory Memorandum to the Bill states

the risk of harm must be real, that is, not remote, for it to give rise to a serious data breach. It is not intended that every data breach be subject to a notification requirement. It would not be appropriate for minor breaches to be notified because of the administrative burden that may place on entities, the risk of 'notification fatigue' on the part of individuals, and the lack of utility where notification does not facilitate harm mitigation.

Finance considers that a payslip for a single individual sent to another individual may well be considered a serious data breach. This is because there is a real risk of harm if the payslip includes bank account details, address details and other personal details. Finance considers that the requirement to notify the OAIC of these single instances of single serious data breaches may lead to notification fatigue for agencies and organisations. In addition, it is not clear what purpose the notification to the OAIC is in these cases. Very little information has been provided on why the OAIC wants this information and what the OAIC will do with the information once it is received.

Finance notes the principles of the recommendations made in the *Independent Review of Whole-of-Govenment Internal Regulation (Belcher Red Tape Review)* (Red Tape Review) available at http://www.finance.gov.au/publications/reducingredtape/ . In particular, the terms of reference for the Red Tape Review provided that the *over-arching principle* for the review *is that regulators prove that regulation is needed*[1]. In addition, the report stated in relation to regulation:

- *the minimum needed to achieve policy (or entity) outcomes.*
  - *Regulation should be created only where, in comparison to other options, it is justified by an analysis of the burden to be imposed against the benefits for policy outcomes or entity performance.*

Finance notes that legislation that applies beyond the public sector, such as privacy legislation, was beyond the scope of the Red Tape Review. However, Finance considers that all new regulation should be consistent with government policy and in particular the overall principles of reducing red tape by only imposing the minimum amount of regulation needed to achieve a policy outcome.

Finance considers that consistent with the ALRC report and the Red Tape Review it would be appropriate to require data breach notification to the individual in all cases of a serious data

[1] Engagement of Independent Reviewer - Terms of Reference, page 2 http://www.finance.gov.au/publications/reducingredtape/ accessed on 2 March 2016

breach. Using the example given above (a single payslip sent to the wrong individual) it would clearly be appropriate to notify the individual so they could take necessary steps to change bank details etc to protect from economic loss. However, Finance considers that in such cases notification to the OAIC should not be required.

Finance notes in the international examples given, that the United States (California) has a two-tier notification system. That is, notification to an individual is required if their unencrypted personal information is acquired without authority. However, notification to the Attorney General is only required if the data breach affects more than 500 individuals. Finance suggests a two-tier system where notification to the OAIC is only required if there is a large scale data breach (such as a breach that affects more than 500 individuals), which would be consistent with both the ALRC report and the Red Tape Review.

Thank you for the opportunity to provide submissions in relation to this matter. If you would like to discuss the principles of the Red Tape Review further, the responsible area in Finance would be happy to meet with you to discuss.