Australian Government
Attorney-General's Department

Deputy Secretary

Civil Justice and
Legal Services Group

Mr Jason McNamara
Executive Director
Office of Best Practice Regulation
Department of the Prime Minister and Cabinet
One National Circuit
BARTON ACT 2600

Email: helpdesk@obpr.gov.au

Dear Mr McNamara

Regulation Impact Statement for early assessment

I am writing in relation to the attached Regulation Impact Statement (RIS) prepared for Privacy Amendment (Notification of Serious Data Breaches) Bill 2015.

I believe the RIS meets best practice requirements and is consistent with the ten principles for Australian Government policy makers.

The RIS answers the first four of the seven RIS questions, and sets out a planned consultation process.

In particular, the RIS addresses the first four RIS questions:

- What is the problem? – with advances in technology, entities subject to the *Privacy Act 1988* are storing larger amounts of identifying information electronically, leading to an increased risk of a security breach. According to research cited in the RIS, data breaches impose substantial costs on businesses and can lead to losses for individuals such as theft or identity fraud.
- Why is government action needed? – Although entities subject to the Privacy Act must already comply with information security requirements in the Act, they are not required to notify affected individuals following a data breach.
- What policy options are you considering? – The RIS considers the following options:
    - Option One (non-regulatory option): retain the status quo. Data breach notification would continue to be voluntary. Individuals would only receive notification if the entity decides to do so.
    - Option Two: amend the Privacy Act to include a mandatory data breach notification scheme for serious data breaches.
    - Option Three: encourage industry to develop industry codes for data breach notification under the Privacy Act.
- What is the likely net benefit of each option? –

- Option One: no change compared to current arrangements in terms of benefits for individuals; businesses would avoid cost of a mandatory data breach notification scheme.
- Option Two: individuals would be notified of a serious data breach involving their personal information; businesses would have greater incentive to comply with existing Privacy Act information security requirements to avoid serious data breaches occurring.
- Option Three: industries which choose to develop codes could develop data breach notification schemes tailored to their own particular industry sector.

In addition:

- changes have been made to the RIS in response to advice received from OBPR on 20 and 21 August 2015 to ensure is the RIS meets best practice requirements;
- the change in regulatory burden on business, community organisations and/or individuals has been quantified using the Regulatory Burden Measurement framework and officer level communication has confirmed OBPR agrees with the initial estimates;
- AGD proposes that the regulatory impact of this measure be offset against the regulatory savings achieved through the implementation in 2015 of Privacy Determinations relating to International Money Transfers (Reference number ZAGD0001-RC1).); and
- an appropriate consultation plan is described.

I resubmit the certified RIS to the Office of Best Practice Regulation for early assessment, consistent with best practice.

Yours sincerely

Matt Minogue
A/g Deputy Secretary
Civil Justice and Legal Services Group
Attorney-General's Department
24 August 2015