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)*	PayPal Australia Simon Edwards Director of Government Relations
Contact details *(one or all of the following: postal address, email address or phone number)*	[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The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.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

PayPal provides payment services for consumers and merchants to send and receive payments in a secure manner and without sharing sensitive payment information.

PayPal has operated in Australia for more than 10 years and was one of the first 'digital wallets' to aim to provide fast, safe, simple and secure transactions for consumers and merchants. Our payments platform, fraud prevention tools and extensive risk management capabilities make PayPal extremely secure.

PayPal processes every year more than 1 billion transactions globally. To successfully deliver these payments PayPal collects, secures and manages millions of pieces of digital data concerning our customers and their accounts. Protecting this data from data breaches, both deliberate and inadvertent, is a key priority for PayPal.

Customers expect that their personal information held by service providers will be used for the purpose for which it was provided, it will be used to provide a benefit to them and it will be secured and maintained only for those purposes.

PayPal welcomes the Government's proposal to legislate for the notification of serious data breaches and acknowledges the effort to produce a set of clear rules and an objective reporting standard to guide decision making by organisations in circumstances where those organisations confront a data breach. Globally, the problem of data breaches and attempts to breach data has been increasing in recent years. There has been a long debate in Australia on the value of a mandatory data breach law and PayPal agrees that there are sound and pressing reasons for a comprehensive national law.

PayPal notes that the goal of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015* is to allow individuals whose personal information has been compromised by a breach to take remedial steps to lessen the adverse impact upon them that might arise from the breach. To achieve this goal the Bill imposes on organisations a mandatory obligation to inform individuals impacted by breach of data in circumstances where the organisation judges the breach poses a real risk of serious harm to the individual to whom the data relates.

As noted in the Bill's Explanatory Memorandum, the use of a specified harm threshold is not uncommon in international jurisdictions. Such delineation is important as it focuses responses by organisations to data breaches upon the impact of those breaches on those whose data has been held and breached. While this threshold delineation is welcomed it will require organisations to both make predictive assessments about the probability of a harm occurring and will require that they assess that there is a real risk of serious harm being suffered by an individual.

PayPal recognises that the alternative to the proposed scheme would be a comprehensive disclosure of all data breaches regardless of their impact on individuals. Such a policy would have potentially far reaching consequences including 'breach fatigue' which may lead consumers to fail to act in their own interests in the event of a serious breach.

For the reasons outlined by the ALRC in its Report 108, PayPal supports limiting the reporting regime to data breaches involving a real risk of serious harm. However, for the reasons set out below, the framing of the concepts of "real risk" and "serious harm" in the Bill may have the unintended consequence of stifling the intention of the assessment process in proposed subsection 26WC(2) to "discourage entities from acting out of an abundance of caution to notify a data breach".[1]

[1] Explanatory Memorandum to the Bill at 86.

Harm

Notwithstanding PayPal's support for the limitation of disclosure, we are concerned that the breadth of the harm to which organisations must give consideration is overly broad. In particular, PayPal is concerned that the regime will require organisations to assess characteristics of individuals without any reasonable capacity or basis for doing so. On balance PayPal does not support imposing the obligation on an organisation to consider the real risk of serious harm to an individual's emotional or psychological state or harm to their reputation where the personal information concerned does not have a sufficient connection with emotional, psychological or reputational characteristics of the individual. One way to address this anomaly is to prescribe these types of harm as forming part of an organisation's assessment where the types of information held by the organisation, and breached, are directly related to an individual's emotional or psychological state or their public reputation.

In particular, harm to reputation is in PayPal's view far too vague a concept and indeterminate in its scope to be included in legislation that defines a contravention of Section 26WC or 26WD as an interference with the information privacy, rather than the private life, of an individual.

PayPal notes that the definition of harm in Section 26WF is intended to be inclusive. As such psychological, emotional and reputational harm would be factors expected to be considered by an entity in the event of a data breach regardless of them being listed in Section 26WF. While PayPal understands the intention of the Government is to require organisations to give consideration to the widest possible harm that may result from a data breach, PayPal is concerned that such a breadth of harm imposes an unmanageable risk upon entities such that most if not all data breaches will require notification.

Risk

PayPal notes the guidance provided by the Office of the Australian Information Commissioner (OAIC) in respect of how to evaluate the risks associated with a data breach. In particular PayPal notes that that OAIC recommends that organisations evaluate the relationship between the unauthorised recipients of data and the affected individuals. This recommendation presupposes that the holder of data will know or have the capacity to infer specific characteristics about both the unauthorised recipient of data and the person whose data has been compromised. In addition it anticipates that the nature of the relationship between the recipient of the data and the affected individual will be apparent. While this may in some circumstances be the case it will not always, or commonly, be so.

Other matters

For clarification, PayPal suggests that the term 'information' in Section 26WB(2)(a) of the draft bill be defined to mean personal information as referenced in Section 26WB(1).

PayPal further recommends that where, as a result of the operation of Section 26WC(10), the Commissioner issues a written notice to an entity refusing the entity's application pursuant to Section 26WC(8)(b) it would be appropriate, on natural justice grounds, that the Commissioner include in the written notice a summary of the reasons for the Commissioner's refusal.