Dear Colleagues

Exposure Draft: Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (Bill)

The Financial Services Council (FSC) has over 115 members representing Australia's retail and wholesale funds management businesses, superannuation funds, life insurers, financial advisory networks, licensed trustee companies and public trustees. The industry is responsible for investing more than $2.6 trillion on behalf of 11.5 million Australians. The pool of funds under management is larger than Australia’s GDP and the capitalisation of the Australian Securities Exchange and is the third largest pool of managed funds in the world. The FSC promotes best practice for the financial services industry by setting mandatory Standards for its members and providing Guidance Notes to assist in operational efficiency.

We refer to the Discussion Paper issued in December 2015 and the Exposure Draft of the Bill and Explanatory Memorandum (EM) released with that Discussion Paper. Thank you for the invitation to make a submission on the Bill. We have set out our comments in relation to the material below.

1. General Comments

Updated Guidance Material

The FSC notes that many of the concepts in the Bill are similar to those provided in the following materials previously published by the Office of the Australian Information Commissioner (OAIC):

1. Data breach notification guide: A guide to handling personal information security breaches, dated August 2014; and
2. Consultation draft: Guide to developing a data breach response plan, dated October 2015

We note in item 19 of the Explanatory Memorandum that it is anticipated that the Commissioner will update item 1 above or release other guidance material “to assist entities in
Annual Report of Regulator Activity

The FSC has reviewed the mandatory data breach reporting schemes in other jurisdictions including the United States of America and the United Kingdom and notes that both the Information Commissioner’s Office (ICO) and the California Department of Justice publish annual reports pertaining to data breaches including incident trends and breakdown by sectors such as telecommunications industries, financial service industries etc. These reports include actions that the regulators have taken against entities that have experienced data breaches.

Encryption and other security controls for the transmission of data

“26WB Serious data breach

Relevant Matters

(3) For the purposes of this section, in determining whether there is a real risk of serious harm to an individual as mentioned in 3 subparagraph (2)(a)(i) or (b)(ii), have regard to the following:

[...]

(c) whether the information is in a form that is intelligible to an ordinary person;

(d) if the information is not in a form that is intelligible to an ordinary person—the likelihood that the information could be converted into such a form;

(e) whether the information is protected by one or more security measures;

(f) if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;

(g) the persons, or the kinds of persons, who have obtained, or who could obtain, the information”

We have reviewed the ICO “Notification of PECR Security Breaches – Privacy and Electronic Communications Regulations” and note that it states as follows:

If the personal data was encrypted to an appropriate standard and the decryption key remains secure, service providers should strictly speaking still notify us of the breach. However, the ICO is unlikely to take formal enforcement action against an organisation that fails to notify us of a breach if the information was properly encrypted and remains secure.

Similarly, paragraph 26WB(3) sets out a range of technological considerations that may ultimately decide whether a particular breach warrants notification. In relation to clauses (c)
and (d), we note that paragraphs 42 and 43 of the EM provide examples of information that may not be intelligible to an ordinary person, including ‘encrypted electronic information’.

The inclusion of these matters suggests that there may be an expectation that APP entities will implement a certain level of encryption and other security measures for all forms of data handling.

The FSC recognises that encryption and other security tools are useful for data requiring a higher than normal level of security, however we consider that it would be an unnecessary administrative burden to use an encryption tool for the transmission of all data between entities, customers, business partners and outsourced service providers. Currently financial services providers utilize different encryption and other security controls depending on their size, the nature of the information they hold, the number and nature of transactions processed and the sophistication of their information technology systems.

We would expect that an entity would be deemed to have taken adequate measures if it had in place reasonable encryption and other security controls to protect their customer information against unauthorised access, use or disclosure. This is particularly the case where those controls were applied generally consistently in the industry such as password protection for online banking.

Should the OAIC expect entities to have specific encryption and other security controls we would expect OAIC guidance materials to provide clarity from the OAIC on this issue.

**Online Platform for Notification**

We also note that the ICO document referenced above provides a secure web form for organisations to use to notify the regulator of data breaches and would expect the OAIC to use a similar mechanism.

**Register of Security Breaches**

The ICO document referenced above also stipulates that organisations are required to keep a log of data security breaches including:

- the facts surrounding the breach; and
- the effects of the breach and remedial action taken.

We note that the ICO requires that the log must be sufficient to allow the Information Commissioner to verify compliance with the provisions of the regulations.
Timeframe for notification to align with timeframe for resolving disputes

We note that the 30 day notification within 26WC(2) does not align with the 45 day period required to resolve disputes under requirements which apply to financial services providers under for example Corporations Act EDR regimes (eg, FOS).
2. Specific Comments

“26WC Entity must notify serious data breach

(1) If an entity is aware, or ought reasonably to be aware, that there are reasonable grounds to believe that there has been a serious data breach of the entity, the entity must, as soon as practicable after the entity becomes so aware, or ought reasonably to have become so aware, as the case may be:

(a) prepare a statement that complies with subsection (3); and

(b) give a copy of the statement to the Commissioner; and

(c) take such steps (if any) as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; and

(d) if it is not practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates:

(i) publish a copy of the statement on the entity’s website (if any); and

(ii) take reasonable steps to publicise the contents of the statement.”

2. A. Tiered approach regarding breach notifications

In its “Discussion paper – Mandatory data breach notification” the Attorney-General’s Department notes that the reporting scheme proposed for Australia would be “simpler than many actual or proposed schemes in other jurisdictions, in that it does not contain a two-tier scheme where some kinds of breaches must only be notified to a regulator, and other kinds to both the regulator and affected individuals”.

While acknowledging these points, we are conscious that such a regime is likely to result in over-reporting of relatively trivial, minor, confined and objectively insignificant incidents. This could occur where, for example, an APP entity determines that there has been a serious data breach causing a real risk of serious harm to only one or two individuals.

We agree that APP entities should notify affected individuals of such a breach (regardless of the number of individuals affected), but we query the value to the Privacy Commissioner of receiving such notifications in cases where only a very small number of individuals are impacted.

We note in item 33 of the Explanatory Memorandum that “In order not to impose an unreasonable compliance burden on entities and to avoid the risk of ‘notification fatigue’ among individuals receiving a large number of notifications in relation to non-serious breaches, it is not intended that every data breach be subject to a notification requirement”. The FSC welcomes this pragmatic approach.

Another example is where one individual’s information is lost resulting in a serious data breach, yet it is not practicable for the APP entity to notify this individual. This may occur if the
individual is a former client for whom the APP entity does not have current contact information. In this situation we do not believe it would be appropriate to place a statement on the APP entity’s website, as this would greatly increase the risk of all individuals suffering notification fatigue.

On the expectation that OAIC will implement an online notification platform for breach reporting, we anticipate that a tiered approach could be implemented with a range of reporting ‘tiers’, with each tier representing a breach with different characteristics. For example, tiers could be allocated on the basis of the number of affected individuals, the nature of the information lost or disclosed or the period of time that has elapsed since the breach (see 2.B below). Additionally, it may be appropriate for some of these tiers to be non-reporting tiers.

Given limited OAIC resources, such an approach would allow OAIC to easily identify (and promptly respond to) those breaches carrying the greatest risk of harm for the greatest number of individuals.

In this regard, a tiered-approach need not introduce additional complexity and would promote ‘effectiveness’ of reporting, reducing the administrative burden on both the OAIC and APP entities.

Recommendation 1: We recommend that a simple tiered approach be considered, along with effective ways of implementing such an approach.

2. B. Identification of a serious data breach in circumstances where significant time has elapsed since the breach occurred

It is understood that entities are expected to have operational controls in place to identify, manage and report serious data breaches. However, in some cases, breaches may not be identified for a significant amount of time after they occurred. For example, an internal or external audit conducted on an entity may identify a breach that occurred a year earlier.

In circumstances where there are likely to be no adverse consequences for individuals and the entity has notified the OAIC and taken all reasonable steps to fix the issue, there may be limited value in notifying the impacted customers. Notification may also be detrimental if it causes them unnecessary concerns.

Conversely, we understand that it may be difficult to adequately consider whether any individuals have suffered, or are likely to suffer, any adverse consequences from a breach. This is particularly the case where cyber criminals may derive a larger benefit by waiting to take advantage of lost or disclosed information. In these cases, individuals may still benefit from notification.

We also note that, in some cases, the risk of harm at the time of the breach may have been assessed as a ‘real risk of serious harm’ (had the entity been aware of it) and with the passage of time and more information at its disposal, the entity may now determine that there was
actually no real risk of serious harm when the breach occurred. It therefore follows that there was no serious data breach and consequently no requirement to report.

Recommendation 2: The FSC recommends that the OAIC provides additional guidance regarding the obligations of APP entities in such de minimis circumstances and that the final legislation addresses the issues described above.

2. C. Obligation to be aware of serious data breach

The current drafting of proposed Section 26WC(1) introduces an objective test whereby an APP entity may be caught by the notification requirements where that entity “ought reasonably to be aware” of reasonable grounds suggesting a breach.

In its current form, it is not clear whether an APP entity can immunise itself from being caught by this test by establishing that it has taken reasonable steps, or implemented reasonable controls, to ensure that it becomes aware of any grounds suggesting a breach.

Depending on the operational controls, IT systems and sophistication of the entity it may be easy for an organisation to become aware of a serious data breach; however, there are circumstances where it may be extremely difficult for an organisation to be aware of a data breach. Examples of this include, but are not limited, to the following:

- Trusted insider risk where an existing or ex-employee has access to customer data;
- Visitors to offices inadvertently accessing customer data;
- Employees accessing or disclosing personal information outside the requirement or authorisation of their employment;
- Mistakenly providing personal information to the wrong person e.g. by sending out account or policy details to the wrong postal or email address;
- Improperly providing personal information to an unauthorised person by being deceived by an individual into divulging that information;
- Paper files, laptops and removable storage devices being lost or stolen when they contain personal information;
- Hard disk drives and other digital storage media being disposed of or returned to equipment lessors without the contents first being erased;
- Databases being hacked into or otherwise illegally accessed by individuals outside the organisation; and
- Paper records stolen from insecure recycling or waste bins.

The methods used by cyber criminals to hack into the IT systems of entities are becoming increasingly sophisticated and are often aimed to avoid detection. The FSC expects that entities would conduct a risk assessment of the controls it has in place to prevent serious data breaches and would implement appropriate operational controls such as those listed in the Guidelines to Australian Privacy Principle 11.
Recommendation 3: We recommend that the legislation reflect that entities which have taken all reasonable steps to ensure they become aware of serious data breaches will not be in breach, particularly as it is logistically impossible to be aware of all serious data breaches.

“26WB Serious data breach

Serious data breach

(2) If:

(a) there is unauthorised access to, or unauthorised disclosure of, the information, and:
   (i) the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the information relates; or
   (ii) any of the information is of a kind specified in the regulations; or

(b) the information is lost in circumstances where:
   (i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and:
   (ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the information relates; or

(c) the information is lost in circumstances where:
   (i) unauthorised access to, or unauthorised disclosure of, the information may occur, and:
   (ii) any of the information is of a kind specified in the regulations;

the access or disclosure covered by paragraph (a), or the loss covered by paragraph (b) or (c), is a serious data breach of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be.”

2. D. Likely impact of harm on the impacted individual/s

Conceptually, where there has been unauthorised access to, or disclosure of, information, the section requires the seriousness of harm to be considered in the context of potentially affected individuals. The concept of ‘harm’ is further defined in section 26WF to include psychological, emotional and reputational harm (among others).

Such concepts can be highly subjective, depending upon the ‘individual’ concerned.

For example, a customer who, unknown to the provider, is subject to serious mental health issues may be more likely to exaggerate the emotional harm that they consider has been the result of a privacy data breach. By contrast, a reasonable person may consider that is only a minor issue and that the entity had taken all reasonable steps to rectify the matter.
We note that in many cases, a financial services organisation would have no visibility regarding the mental health status of its customers.

Recommendation 4: We submit that further clarity and guidance to assist in the practical application of these concepts would be appropriate.

2. E. ‘Individuals’ to be treated as a group in certain cases

We submit that it would be impossible in most cases for the entity to consider the impact on “...any of the individuals to whom the information relates...” if that is to be taken as a reference to discrete individuals one by one.

For example, if a data breach involved many thousands of customer records, the entity could not reasonably assess the likely impact on the psychological, emotional and reputational health of several thousand individuals one by one. Necessarily, an assessment will have to be made on a more generalised basis across the group of individuals affected.

Recommendation 5: We submit that the concept of ‘individuals’ should be expressly qualified such that an entity is to consider the likelihood of harm to the affected group of individuals, as the circumstances reasonably require.

2. F. Individuals with particular risk characteristics

Where a data breach involves information that puts a single individual at particular risk, and that individual has taken all necessary steps to ensure that they are actually known to the entity to be at a particular risk of harm, then it may be reasonable in some cases for the entity to consider that person on an individual basis. An example would be where an individual has notified the entity of a domestic violence situation. In this case the entity may be expected to be aware of the additional risks of allowing that individual’s residential address to be disclosed in a manner that may bring it to the attention of a threatening person.

In cases such as this, we note that individual responsibility is required. An entity can reasonably be expected to consider the particular needs of the individual only if the entity has been formally put on notice of them. For example, being put ‘on notice’ would take more than a conversation with a bank teller. Some formal step would have to be taken by the individual in question to cause the entity to record that individual’s circumstances.

**Scenario:**

A file containing customer records concerning about 1000 customers is disclosed to an unauthorised recipient. The data includes the customer’s name, date of birth, postal and email addresses, health information for an application for insurance and financial information to process a transaction such as a premium payment or investment. A financial services provider would be unlikely to know the following in the course of their general transactions with the customer to provide banking, insurance or investment products and services to those customers:
One of the customers has an Apprehended Violence Order against family members and is currently in fear of others threatening their life or physical security. This particular customer would be more concerned about harm as a consequence of the disclosure.

One of the customers is currently in a witness protection program and is currently in fear of others threatening their life or physical security. This particular customer would be more concerned about harm as a consequence of the disclosure.

Unless a customer or someone with the customer’s authority, acting on their behalf, contacts the financial services provider to notify it of the customer’s particular circumstances, we consider that it would be unreasonable to assume that the APP entity was aware of the specific serious risk of harm to that individual.

Given the above:

- An entity should only be required to consider the needs of a particular individual where that individual has taken all necessary steps to put the entity on notice of those particular circumstances and it was reasonable in all the circumstances for the entity to consider those circumstances.

- We submit that it would be inappropriate to expose an entity to the risk of legal action by a specific individual, on the basis of a specific characteristic of that individual, where the entity did not actually know of that specific characteristic and how it may lead to a particular risk of harm.

- The same is true of classes of individuals who may have rights to pursue class actions.

We note that whilst the intention is for the more serious enforcement remedies, such as civil penalties, to be imposed only for serious or repeated interferences with privacy (see the EM at paragraph 16), in certain circumstances it may still be possible for affected individual(s) to pursue a pecuniary remedy in a private action, including through a class action.

**Recommendation 6: The legislation should be drafted to limit such exposures.**

2. **G. Interpretation of ‘individual’**

We note that section 26WB(3)(c) expressly applies an objective test by using the phrase ‘ordinary person’. The distinction between ‘ordinary person’ and ‘individual’ is a factor that would imply the correct legal interpretation of ‘individual’ is subjective on a case by case basis. As noted above, we submit that this would be inappropriate in most circumstances.

**Recommendation 7: We suggest that consideration be given to recasting the legislation in this respect so that it focuses more on objective circumstances and the actions which an entity might reasonably be expected to take in those circumstances.**
2. H Practical considerations where data is lost

Where data is lost, (proposed section 26WB(2)(b)), the entity is required to:

- first consider whether unauthorised access/disclosure is "likely to occur"; and
- then (on the assumption that unauthorised access/disclosure will occur), whether serious harm to an individual will result.

We submit that such an exercise involves real difficulty in practice, building as it does an assumption that depends upon a prior assumption. That is to say, in order to assess whether serious harm to an individual will occur, an entity must not only assume unauthorised access/disclosure – it must also make assumptions as to whom/where that unauthorised access/disclosure has occurred.

Recommendation 8: We submit that further guidance would be valuable in this regard. It also reinforces the need for a defence to be built in to the legislation as set out below.

2. I. Defence of reasonable steps

Consistently with the comments we have made above, particularly in 2. C and 2. D, we submit that consideration should also be given to the need for a defence of ‘reasonable steps’ or a similar concept. Where an entity has taken such steps as are reasonable in the circumstances to determine whether a data breach is a ‘serious data breach’ that should form a defence against an allegation that a particular individual’s risk of serious harm was not foreseen.

Recommendation 9: We submit that consideration be given to a general defence of ‘reasonable steps’ and an overarching filter of objectivity applied in the final legislation for matters such as these.
“26WB Serious data breach
Overseas recipients
(5) If:

(a) an APP entity has disclosed personal information about one or more individuals to an overseas recipient; and

(b) Australian Privacy Principle 8.1 applied to the disclosure of the personal information; and

(c) the overseas recipient holds the personal information;

this section has effect as if:

(d) the personal information were held by the APP entity; and

(e) the APP entity were required under section 15 not to do an act, or engage in a practice, that breaches Australian Privacy Principle 11.1 in relation to the personal information.”

2. J. Overseas aspects

Proposed Section 26WB(5)(c) refers to disclosure of personal information to overseas recipients. It is unclear to us how this “fits” with existing APP 8.1 requirements when there are international aspects to the data breach.

Recommendation 10: The FSC recommends that the OAIC provides additional guidance regarding the notification of serious data breaches where there are cross-jurisdictional issues.

2.K Notification of individual where such notification would be inconsistent with the law of a State or Territory

Sub-section 26WC(12) provides that if compliance by an entity with paragraph 26WC(1)(b), (c) or (d) would, to any extent, be inconsistent with a provision of a law of the Commonwealth (other than a provision of this Act) that prohibits or regulates the use or disclosure of information, subsection (1) does not apply to the entity to the extent of the inconsistency.

There are numerous State and Territory laws which may prohibit or regulate an entity’s use or disclosure of information in a given case. Examples include relevant provisions in ombudsman, whistleblower, and anti-corruption legislation. It would not be appropriate for an entity to give notification to an individual in breach of such laws, nor would it be appropriate for an entity to be in the position of having to assess the constitutional issue as to whether the Commonwealth notification law overrides such a State or Territory law.
Where provision of notification to an individual would be inconsistent with such a law, the entity should be able to comply with section 26WC(1) **solely** by notifying the Commissioner (not the individual).

**Recommendation 11:** The FSC recommends that the legislation include an additional exemption to section 26WC(1) under which, if compliance by an entity with paragraph 26WC(1)(c) or (d) would, to any extent, be inconsistent with a provision of a law of a State or Territory that prohibits or regulates the use or disclosure of information, that paragraphs 26WC(1)(c) and (d) do not apply to the entity to the extent of the inconsistency.

**2. L. Notification of individual where the entity is aware that the individual is under a legal disability**

Particular difficulties may arise where an entity is acting for an individual who, by reason of a disability, is unable to manage their affairs. For example, the individual may have severe dementia, and the entity may have responsibility for administering their financial and property affairs (in whole or in part) under an enduring power of attorney or similar instrument, or under an appointment by a Court or Tribunal. The individual’s disability may be such that they would be unable to understand any notification given to them by the entity under s26WC(1)(b), and would be unable to take any of the recommended steps set out in the notification statement. (In some cases, it may indeed be that the entity itself is responsible for taking such steps, in the individual’s best interests, on that individual’s behalf; for example, if the entity is the individual’s financial attorney, manager or administrator.)

In such cases, the notification requirement under s 26WC(1)(b) would be of no use or benefit to the individual. On the contrary, receipt of such notification may cause the individual distress or, potentially, harm, without having any compensatory beneficial purpose. Whilst it would be open to the entity to apply to the Commissioner for an exemption under paragraph 26WC(8)(b), this would be administratively burdensome, and it is not clear that the Commissioner would have the expertise to determine a course that would be in such an individual’s best interests. The entity may be able to apply to the relevant State/Territory body for advice and direction: State/Territory tribunals and courts with oversight of the administration of the affairs of individuals with a disability have greater specialist expertise and experience than the Commissioner in determining what is in such individuals’ best interests. If it is more likely that an individual’s receipt of notification pursuant to s 26WC(1)(b) would be detrimental, rather than beneficial, to that individual, it is arguably inherently unreasonable for the entity to provide such notification; however, this conclusion is not clear cut on the face of the draft provision.

**Recommendation 12:** The FSC recommends that the legislation exempt circumstances where the entity is aware that, due to disability, the individual would derive no benefit from a
notification, and where notification would pose a risk of causing distress or other harm to the individual.

Please contact Paul Callaghan on [redacted] if you have any questions on our submission.

Yours Faithfully

Paul Callaghan
General Counsel